CA ARCserve® Central Protection Manager

Benutzerhandbuch

r16

Diese Dokumentation, die eingebettete Hilfesysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von CA jederzeit geändert oder zurückgenommen werden.

Diese Dokumentation darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden. Diese Dokumentation enthält vertrauliche und firmeneigene Informationen von CA und darf vom Nutzer nicht weitergegeben oder zu anderen Zwecken verwendet werden als zu denen, die (i) in einer separaten Vereinbarung zwischen dem Nutzer und CA über die Verwendung der CA-Software, auf die sich die Dokumentation bezieht, zugelassen sind, oder die (ii) in einer separaten Vertraulichkeitsvereinbarung zwischen dem Nutzer und CA festgehalten wurden.

Ungeachtet der oben genannten Bestimmungen ist der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt(e) verfügt, berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT CA DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN CA ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Software-Produkte unterliegt den entsprechenden Lizenzvereinbarungen, und diese werden durch die Bedingungen dieser rechtlichen Hinweise in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Zur Verfügung gestellt mit „Restricted Rights“ (eingeschränkten Rechten) geliefert. Die Verwendung, Duplizierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absätze 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227-7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Nachfolgebestimmungen.

Copyright © 2012 CA. Alle Rechte vorbehalten. Alle Marken, Produktnamen, Dienstleistungsmarken oder Logos, auf die hier verwiesen wird, sind Eigentum der entsprechenden Rechtsinhaber.

CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA Technologies:

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication and High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

CA Kontaktieren

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Support-Links für CA ARCserve Central Applications:

CA Support Online stellt eine Vielfalt an Ressourcen zur Lösung von technischen Problemen zur Verfügung und bietet einfachen Zugriff auf wichtige Produktinformationen. Mit CA Support haben Sie zu jeder Zeit schnellen und einfachen Zugang zu vertrauenswürdigen Auskünften. Über die folgenden Links gelangen Sie zu den unterschiedlichen CA Support-Seiten, die Ihnen zur Verfügung stehen:

- **Informationen zum Support**: Über diesen Link erhalten Sie Informationen zu Wartungsprogrammen und Support-Angeboten sowie zu Bedingungen, Rechtsansprüchen, Service Level Objectives (SLO) und Servicezeiten.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Registrierung für Support**: Dieser Link führt Sie zum CA Support Online-Registrierungsformular, mit dem Sie Ihren Produkt-Support aktivieren können.

  https://support.ca.com/prodinfo/supportregistration

- **Technischer Support**: Die folgende Verknüpfung führt Sie zur One-Stop Product Support-Seite für CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Änderungen in der Dokumentation

Das Dokument enthält Benutzer-Feedback, Verbesserungen, Korrekturen und andere kleinere Änderungen, um die Verwendung und das Produktverständnis oder die Dokumentation selbst zu verbessern.

Seit der GA-Version dieser Dokumentation wurden folgende Aktualisierungen der Dokumentation vorgenommen:

Aktualisierung 7

- Das Thema Zusammenführungsjob-Optionen (siehe Seite 70) wurde hinzugefügt. Dieses Thema enthält zwei neue Optionen auf der Knotenansicht: Zusammenführungsjob unterbrechen (siehe Seite 71) und Zusammenführungsjob wiederaufnehmen (siehe Seite 72). Diese Themen beschreiben, wie sie einen Zusammenführungsjob für einen bestimmten Knoten unterbrechen oder wiederaufnehmen.
- Das Thema So legen Sie Schutzeinstellungen fest (siehe Seite 89) wurde aktualisiert. Dieses Thema enthält Informationen zu den Optionen der Aufbewahrungseinstellungen. Mit den Aufbewahrungsrichtlinien geben Sie die Anzahl der aufzubewahrenden Wiederherstellungspunkte oder der aufzubewahrenden Wiederherstellungssätze an.
- Das Thema So legen Sie E-Mail-Warnungen fest (siehe Seite 127) wurde aktualisiert. Dieses Thema enthält Aktualisierungen zu den Sicherungswarnungen für Zusammenführungsjobs. Sie können jetzt eine Warnmeldung für Zusammenführungsjobs erhalten, die angehalten oder übersprungen wurden bzw. fehlgeschlagen oder abgestürzt sind. Außerdem wurde eine neue Option hinzugefügt, die Sie auf erfolgreiche Zusammenführungsjobs hinweist.

Aktualisierung 6

- Der Abschnitt Konfigurieren von Discovery-Ablaufplänen (siehe Seite 36) wurde aktualisiert. Dieser Abschnitt enthält jetzt eine Active Directory-Liste, die angezeigt wird, wenn Sie einen Ablaufplan zur Erkennung von Knoten einrichten.
- Der Abschnitt Konfigurieren von E-Mail- und Alert-Einstellungen (siehe Seite 36) wurde aktualisiert. Der Titel wurde geändert und der Abschnitt wurde aktualisiert, um Warnungen bei erkannten Knoten zu berücksichtigen.
- Der Abschnitt Aktualisieren von Knoten (siehe Seite 66) wurde aktualisiert. Das Thema beschreibt, wie Sie gleichzeitig mehrere Knoten aktualisieren können, sei es mithilfe der vorhandenen Anmeldeinformationen oder indem Sie neue Anmeldeinformationen angeben. Sie können auch den Server zwingen, die ausgewählten Knoten zu verwalten.
- Der Abschnitt Knotengruppen hinzufügen (siehe Seite 77) wurde aktualisiert. Dieser Abschnitt ersetzt die "nicht zugewiesene" Knotengruppe durch "Knoten ohne Richtlinie" und die "nicht gruppierte" Knotengruppe durch "Knoten ohne Gruppe".

- Der Abschnitt Bereitstellen von CA ARCserve D2D auf Knoten (siehe Seite 84) wurde aktualisiert. Der Abschnitt wurde aktualisiert, um die neueste CA ARCserve D2D-Version bei der Bereitstellung auf Knoten zu berücksichtigen, sowie zur Unterstützung früherer CA ARCserve D2D-Versionen. Der Abschnitt behandelt auch eine neue Schaltfläche namens "Alle Knoten der Bereitstellungsliste auswählen bzw. die Auswahl aufheben".
- Der Abschnitt So legen Sie Dateikopieziele fest (siehe Seite 113) wurde aktualisiert. Der Abschnitt wurde aktualisiert, um Fujitsu Cloud (Windows Azure) als einen weiteren Anbietertyp für Cloud-Konfiguration einzubeziehen.
- In dieser Aktualisierungsversion können Sie jetzt den Status einer Richtlinienbereitstellung in der Richtlinien-Spalte anzeigen.

Aktualisierung 5

- Aufbau des Fensters "Knotenverwaltung" (siehe Seite 58). Der Screenshot der Knotenansicht wurde aus diesem Thema entfernt, da die Benutzeroberfläche fortlaufend geändert wurde.
- Hinzufügen von Knotengruppen (siehe Seite 77). Dieses Thema wurde aktualisiert, um die Filter "Gruppe" und "Knotenname" hinzuzufügen.
- Bereitstellen von CA ARCserve D2D auf Knoten (siehe Seite 84). Dieses Thema wurde aktualisiert, um dem Bildschirm "D2D-Bereitstellung" den Filter "Gruppe" und "Knotenname" hinzuzufügen.
- Zuweisen und Aufheben der Zuweisung von Knoten aus Richtlinien (siehe Seite 140). Dieses Thema wurde aktualisiert, um dem Bildschirm "Zuweisung der Richtlinie durchführen/aufheben" den Filter "Gruppe" und "Knotenname" hinzuzufügen.

Aktualisierung 4

- So deinstallieren Sie CA ARCserve Central Protection Manager (siehe Seite 23) wurde hinzugefügt. Dieses Szenario beschreibt die Methoden, die Sie verwenden können, um die Anwendung zu deinstallieren.
- Das Thema "Verwenden von CA ARCserve Central Protection Manager zur Sicherung von CA ARCserve D2D-Knoten" (siehe Seite 50) wurde hinzugefügt. Dieses Szenario beschreibt, wie eine grundlegende Sicherungsrichtlinie erstellt werden kann, um CA ARCserve D2D-Knoten zu sichern.
- Das Thema "Sicherung jetzt ausführen" (siehe Seite 141) wurde hinzugefügt. Dieses Thema beschreibt, wie ein Ad-Hoc-Sicherungsjob ausgeführt wird.
- Das Thema "Anzeigen von Jobstatusinformationen" (siehe Seite 143) wurde hinzugefügt. Dieses Thema beschreibt, wie über laufende Sicherungsjobs Informationen in Echtzeit angezeigt werden können.
- Es wurden alle Themen aktualisiert, die beschreiben, wie Sie Daten wiederherstellen (siehe Seite 144) können. Sie übergeben Wiederherstellungsjobs nun direkt vom Fenster "Knoten" aus.
- Das Thema "Ändern des Server-Kommunikationsprotokolls" (siehe Seite 168) wurde hinzugefügt. Dieses Thema beschreibt, wie das von den CA ARCserve Central Applications-Komponenten verwendete Kommunikationsprotokoll mithilfe einer Batch-Datei von HTTP in HTTPS und von HTTPS in HTTP geändert wird.

Aktualisierung 1

- Das Thema Integrieren von CA ARCserve Central Protection Manager-IT-Verwaltungsserver-Tools (siehe Seite 171) wurde hinzugefügt. Dieser Abschnitt beschreibt, wie CA ARCserve Central Protection Manager mit Tools zur Verwaltung der Infrastruktur von IT-Verwaltungsservern integriert werden kann. Zum Beispiel Nimsoft und Kaseya.

Inhalt

Kapitel 1: Einführung in CA ARCserve Central Protection Manager 11

Einführung 11
Funktionsweise der Anwendung 12
CA ARCserve Central Applications-Bookshelf 13

Kapitel 2: Installieren von CA ARCserve Central Protection Manager 15

Erforderliche Installationsaufgaben 15
Installationshinweise 17
Installieren von CA ARCserve Central Protection Manager 17
CA ARCserve Central Protection Manager automatisch installieren 21
So deinstallieren Sie CA ARCserve Central Protection Manager. 23
    Deinstallieren von CA ARCserve Central Protection Manager 25
    CA ARCserve Central Protection Manager automatisch deinstallieren 26
    Richtlinienkontrolle auf die CA ARCserve D2D-Knoten anwenden 27
Auswirkungen des Installationsprozesses auf das Betriebssystem 28
    Binärdateien mit unrichtigen Informationen zur Dateiversion 30
    Binärdateien ohne eingebettetes Manifest 30
    Binärdateien mit "Require Administrator"-Berechtigungen im Manifest 31

Kapitel 3: Erste Schritte mit CA ARCserve Central Protection Manager 33

Sicherstellen, dass der CA ARCserve Central Protection Manager-Server mit den Knoten kommunizieren kann 34
Konfigurieren von CA ARCserve Backup-Datensynchronisations-Ablaufplänen 34
Konfigurieren von SRM-Ablaufplänen 35
Konfigurieren von Discovery-Ablaufplänen 36
Konfigurieren von E-Mail- und Alert-Einstellungen 36
Konfigurieren der Einstellungen von IT-Verwaltungsservern 38
Konfigurieren von Ablaufplänen für Aktualisierungen von CA ARCserve Central Applications 39
    Proxy-Einstellungen konfigurieren 40
Konfigurieren von Voreinstellungen für Social Networking 41
Ändern des Administratorkontos 42
Konfigurieren der Einstellungen für die Bereitstellung von D2D 43
Konfigurieren der Datenbank 44
CA ARCserve Central Protection Manager-Datenbank erneut erstellen 45

Kapitel 4: Verwenden von CA ARCserve Central Protection Manager 49

Verwenden von CA ARCserve Central Protection Manager zur Sicherung von CA ARCserve D2D-Knoten 50
Hinzufügen von Knoten 51
Grundlegende Richtlinie erstellen 51
Knoten zu Richtlinien zuweisen 56
So verwalten Sie Knoten in CA ARCserve Central Protection Manager 57
Aufbau des Fensters "Knotenverwaltung" 58
Funktionen für Knoten 60
Funktionen für Knotengruppen 77
Mithilfe von Discovery nach Knoten suchen 82
CA ARCserve D2D-Bereitstellungsaufgaben 83
Filtern von Knotengruppen 87
Verwalten von CA ARCserve D2D-Richtlinien 88
Erstellen von Richtlinien 88
Bearbeiten oder Kopieren von Richtlinien 137
Löschen von Richtlinien 138
Bereitstellen von Richtlinien 139
Sicherung jetzt ausführen 141
Anzeigen von Jobstatusinformationen 143
Wiederherstellen von Knoten in CA ARCserve Central Protection Manager 144
Wiederherstellen von Daten aus Wiederherstellungspunkten 145
Wiederherstellen von Daten aus Dateikopien 148
Wiederherstellen von Daten aus Dateien und Ordnern 152
Wiederherstellen von Daten von virtuellen Rechnern 155
Wiederherstellen von Microsoft Exchange-E-Mail-Daten 160
Anzeigen von CA ARCserve Central Protection Manager-Protokollen 164
Links zur Navigationsleiste hinzufügen 166
Best Practices 167
Ändern des Server-Kommunikationsprotokolls 168

Kapitel 5: CA ARCserve Central Protection Manager mit IT-Verwaltungsserver-Tools integrieren 171

Integration von CA ARCserve Central Protection Manager mit Nimsoft und Kaseya 171
So integrieren Sie CA ARCserve Central Protection Manager mit Nimsoft 173
Installieren des Roboters 174
Konfiguration von CA ARCserve Central Protection Manager-Servern für die Kommunikation mit Nimsoft-Servern 175
Konfigurieren des Nimsoft Servers für das Erkennen und Versenden von E-Mail-Nachrichten 176
Anzeigen von Informationen über Alerts in "Nimsoft Alarm SubConsole" 176
So integrieren Sie CA ARCserve Central Protection Manager mit Kaseya 178
Installieren des Kaseya-Agenten 179

Konfigurieren Sie den CA ARCserve Central Protection Manager-Server so, dass er mit dem Kaseya-Server kommuniziert. 180
Konfigurieren Sie den Protokoll-Parser für den Kaseya-Server. 181
Zuweisen des Parser-Sets auf dem Kaseya-Server 184
Konfigurieren Sie Kaseya-Server so, dass E-Mail-Nachrichten erkannt und gesendet werden. 186
Informationen zu Alerts im Protokoll-Überwachungsserver des Kaseya-Agenten anzeigen 187

Kapitel 6: Fehlerbehebung in CA ARCserve Central Protection Manager 189

Beim Hinzufügen von Knoten zeigt eine Fehlermeldung an, dass keine Verbindung zum angegebenen Server möglich ist. 190
Leere Webseiten oder JavaScript-Fehler treten auf 192
Bei Anmeldung in CA ARCserve D2D-Knoten laden sich Webseiten nicht richtig 194
Beim Hinzufügen von Knoten werden ungültige Anmeldeinformationen angezeigt. 195
Meldungen zu ungültigen Anmeldeinformationen unter Windows XP 196
Fehler wegen verweigerten Zugriffs beim Hinzufügen eines Knotens nach IP/Namen 197
Beim Anmeldung in der Anwendung wird ein Zertifikatsfehler angezeigt. 199
Fehler beim CA ARCserve Backup-Synchronisationsvorgang 201
Fehlschlagen von Vorgängen zur erneuten Bereitstellung von CA ARCserve D2D 202
Beheben von Problemen beim Laden von Seiten 203
Störzeichen werden in Browser-Fenstern angezeigt, wenn man auf CA ARCserve Central Applications zugreift. 204
Knoten werden nach einer Namensänderung nicht mehr im Bildschirm "Knoten" angezeigt 205
CA ARCserve Central Protection Manager kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen 206
Nach D2D-Bereitstellung werden Knoten nicht verwaltet 207
So legen Sie Ablaufpläne zum Löschen von Knotendaten fest 207
CA ARCserve Central Applications-Datenbankdienste starten nicht 208
Beim Speichern oder Zuweisen einer Richtlinie auf einen CA ARCserve D2D-Server tritt ein "Multiple Connections"-Fehler auf 209
Datensynchronisations- und Richtlinienbereitstellungsvorgänge schlagen fehl 210
Fehlernummern der Fehlerbehebung 211
Die Verknüpfung zum Hinzufügen neuer Registerkarten wird in Internet Explorer 8 und 9 und in Chrome nicht ordnungsgemäß geöffnet 212
Die Verknüpfung zum Hinzufügen neuer Registerkarten, RSS-Feeds und Social Networking-Feedback werden in Internet Explorer 8 und 9 nicht ordnungsgemäß geöffnet 215
Zeichen aus lokalisierten Servern werden in der Nimsoft UMP-Alarmkonsole als unleserlicher Text angezeigt 216

Index 217

Kapitel 1: Einführung in CA ARCserve Central Protection Manager

Dieses Kapitel enthält folgende Themen:

Einführung (siehe Seite 11)
Funktionsweise der Anwendung (siehe Seite 12)
CA ARCserve Central Applications-Bookshelf (siehe Seite 13)

Einführung

CA ARCserve Central Applications verbindet wichtige Datenschutz- und -Managementtechnologien mit einem Ökosystem von Zielanwendungen, die im Einklang miteinander funktionieren, um sowohl Innen- und Außenschutz als auch das Kopieren, Verschieben und Transformieren von Daten quer durch globale Umgebungen zu ermöglichen.

CA ARCserve Central Applications sind einfach zu verwenden, handzuhaben und zu installieren. Sie bieten Organisationen eine automatische Kontrolle über ihre Informationen, um fundierte Entscheidungen über den Zugriff, die Verfügbarkeit und Sicherheit ihrer Daten auf der Basis des allgemeinen Geschäftswerts zu treffen.

CA ARCserve Central Applications umfasst neben anderen Anwendungen CA ARCserve Central Protection Manager. CA ARCserve Central Protection Manager lässt Sie CA ARCserve D2D- und CA ARCserve Backup-Umgebungen von einem zentralen Speicherort verwalten. Individuelle Anwendungen bieten eingeschränkte Möglichkeiten der Knotenverwaltung, während Sie mit CA ARCserve Central Protection Manager Folgendes ausführen können:

- Einen oder mehrere Knoten hinzufügen
- Knoten vom Active Directory-Server erkennen
- Von einem Hypervisor verwaltete virtuelle Rechner erkennen und hinzufügen
- Die Anwendung auf hinzugefügten Servern erkennen
- CA ARCserve D2D-Richtlinien erstellen und zuweisen
- Wiederherstellungsjob für verwaltetes CA ARCserve D2D übergeben
- Daten von verwalteten CA ARCserve Backup- und CA ARCserve D2D-Servern synchronisieren
- CA ARCserve D2D bereitstellen

Funktionsweise der Anwendung

CA ARCserve Central Protection Manager lässt Sie geschützte Knoten anzeigen und vom zentralen Speicherort verwalten.

Starten Sie CA ARCserve Central Protection Manager über Startmenü > Alle Programme > CA > ARCserve Central Applications > CA ARCserve Central Protection Manager. Die CA ARCserve Central Protection Manager-Startseite wird angezeigt, in der Sie auf alle CA ARCserve Central Protection Manager-Funktion mithilfe der folgenden Navigationsfunktionen zugreifen können:

- **Knoten:** Lässt Sie verschiedene Tools verwenden, um Knoten und Knotengruppen zu verwalten, Knoten zu erkennen, CA ARCserve D2D auf Knoten bereitzustellen, und Daten zu synchronisieren.
- **Richtlinien:** Ermöglicht es Ihnen, CA ARCserve D2D-Richtlinien hinzuzufügen, zu bearbeiten, zu löschen, zu kopieren und zuzuweisen. Diese Funktion zeigt die Richtliniendetails an und ermöglicht es Ihnen, einen Knoten zu seiner entsprechenden CA ARCserve D2D-Richtlinie zuzuweisen oder die Zuweisung aufzuheben.
- **Konfiguration:** Ermöglicht es Ihnen, die Einstellungen für die Datenbank, CA ARCserve Backup-Datensynchronisation, SRM, Discovery, E-Mail-Konfiguration, Konfiguration der Aktualisierung, Voreinstellungen, Administratorkonto, D2D-Bereitstellung und IT-Verwaltungsserver zu konfigurieren.
- **Protokolle anzeigen:** Ermöglicht es Ihnen, Aktivitätsprotokolle für alle individuellen Knoten anzuzeigen. CA ARCserve Central Protection Manager zeigt alle Protokollmeldungen an, die diesem Knoten zugeordnet sind. Sie können die Liste filtern, indem Sie den Schweregrad der Meldungen (Alle, Information, Fehler, Warnungen oder Fehler und Warnungen), den Modultyp (Alle, Allgemein, Knoten aus Discovery importieren, Knoten aus Hypervisor importieren, Knoten aus Datei importieren, Richtlinienverwaltung, CA ARCserve Backup-Synchronisation, CA ARCserve D2D-Synchronisation, Aktualisierungen für CA ARCserve D2D, Aktualisierungen und Übergeben von CA ARCserve D2D- Sicherungsjobs) oder den Knotennamen angeben.

CA ARCserve Central Applications-Bookshelf

Die Inhalte dieser CA ARCserve Central Applications-Hilfe sind auch als Benutzerhandbuch im PDF-Format verfügbar. Auf die neueste PDF-Version dieses Handbuchs und der Hilfe kann vom CA ARCserve Central Applications-Bookshelf aus zugegriffen werden.

Die Dateien mit CA ARCserve Central Applications-Versionshinweisen enthalten Informationen bezüglich Systemanforderungen, unterstützte Betriebssysteme, Support bei der Wiederherstellung der Anwendung und andere Informationen, die Sie kennen sollten, bevor Sie dieses Produkt installieren. Außerdem enthalten die Versionshinweise eine Liste bekannter Probleme, derer Sie sich bewusst sein sollten, bevor Sie CA ARCserve Central Applications verwenden. Auf die aktuelle Version der Versionshinweise kann vom CA ARCserve Central Applications-Bookshelf aus zugegriffen werden.

Kapitel 2: Installieren von CA ARCserve Central Protection Manager

Dieses Kapitel enthält folgende Themen:

Erforderliche Installationsaufgaben (siehe Seite 15)
Installationshinweise (siehe Seite 17)
Installieren von CA ARCserve Central Protection Manager (siehe Seite 17)
CA ARCserve Central Protection Manager automatisch installieren (siehe Seite 21)
So deinstallieren Sie CA ARCserve Central Protection Manager. (siehe Seite 23)
Auswirkungen des Installationsprozesses auf das Betriebssystem (siehe Seite 28)

Erforderliche Installationsaufgaben

Bevor Sie die Anwendung installieren, führen Sie folgende erforderlichen Aufgaben aus:

- Überprüfen Sie die Versionshinweise. Die Versionshinweise enthalten eine Beschreibung der Systemanforderungen, unterstützten Betriebssysteme und eine Liste der Probleme, die in dieser Version von CA ARCserve Central Protection Manager bekannt sind.
- Prüfen Sie, ob Ihr System die Mindestanforderungen für die Hardware und Software erfüllt, die für die Installation der Anwendung erforderlich sind.
- Prüfen Sie, ob Sie über Administratorrechte oder die entsprechende Berechtigung zum Installieren von Software auf den Computern verfügen, auf denen Sie CA ARCserve Central Protection Manager installieren möchten.
- Prüfen Sie, ob Sie die Benutzernamen und Kennwörter der Computer haben, auf denen Sie die Anwendung, die Sie besitzen, installieren.

- Stellen Sie sicher, dass der Server, auf dem Sie CA ARCserve Central Protection Manager installieren, und die Knoten, auf denen Sie Richtlinien bereitstellen wollen, mithilfe ihrer Hostnamen miteinander kommunizieren können. Um sicherzustellen, dass die CA ARCserve Central Protection Manager-Server und -Knoten miteinander kommunizieren können, gehen Sie wie folgt vor:
  - Pingen Sie vom CA ARCserve Central Protection Manager-Server aus die Knoten mit den Hostnamen der Knoten an.
  - Pingen Sie von den Knoten aus, die Sie schützen wollen, den CA ARCserve Central Protection Manager-Server mit dem Hostnamen des Servers an.
- Mit CA ARCserve Central Protection Manager können Sie CA ARCserve D2D r16 installieren und mithilfe des Bereitstellungsprogramms ein Upgrade von CA ARCserve D2D r15 auf CA ARCserve D2D r16 auf Remote-Knoten durchführen. Um Daten auf den Remote-Knoten mithilfe von CA ARCserve D2D r16 zu sichern, müssen Sie über CA ARCserve D2D-r16-Lizenzen verfügen und die Lizenzen auf den Knoten anwenden. Wenn Sie nach der Installation oder nachdem Sie ein Upgrade auf CA ARCserve D2D r16 durchgeführt haben, die Lizenzen nicht innerhalb von 31 Tagen anwenden, kann CA ARCserve D2D nicht mehr verwendet werden.
- Die CA ARCserve Central Protection Manager-Installationsdatenträger enthalten Microsoft SQL Server 2008 R2 Express Edition, welche die Datenbankanwendung ist, die mindestens erforderlich ist, um die CA ARCserve Central Protection Manager-Datenbank zu unterstützen. Wenn Sie Microsoft SQL Server verwenden wollen, um die CA ARCserve Central Protection Manager-Datenbank zu unterstützen, installieren Sie Microsoft SQL Server auf dem CA ARCserve Central Protection Manager-Server oder einem Remote-Server, bevor Sie CA ARCserve Central Protection Manager installieren. Wenn die Installationsroutine eine Version von Microsoft SQL Server entdeckt, die nicht unterstützt wird, schlägt die Installationsroutine fehl. Weitere Informationen über die unterstützten Microsoft SQL Server-Versionen finden Sie unter Versionshinweise.

Installationshinweise

Bevor Sie CA ARCserve Central Protection Manager installieren, überprüfen Sie die folgenden Installationshinweise:

- Das CA ARCserve Central Applications-Installationspaket installiert ein Modul namens CA ARCserve Central Applications Server. CA ARCserve Central Applications Server ist ein Modul, das allen CA ARCserve Central Applications bekannt ist. Das Modul enthält den Webservice, Binärdateien und Konfigurationen, die CA ARCserve Central Applications miteinander kommunizieren lassen.

  Wenn Sie CA ARCserve Central Applications installieren, installiert das Installationspaket das CA ARCserve Central Applications Server-Modul, bevor es die Produktkomponenten installiert. Wenn es notwendig wird, einen Patch für CA ARCserve Central Applications anzuwenden, aktualisiert der Patch das Modul, bevor er die Produktkomponenten aktualisiert.

- Wenn Sie CA ARCserve D2D auf Remote-Knoten bereitstellen, installiert CA ARCserve Central Protection Manager VMware Virtual Disk Development Kit (VDDK) 1.2.1 auf den Zielknoten. Der Installationsdatenträger von CA ARCserve Central Protection Manager beinhaltet die Setup-Dateien, die für die Installation von VMware Virtual Disk Development Kit (VDDK) 1.2.1 auf dem CA ARCserve Central Protection Manager-Server und auf dem Zielknoten erforderlich sind. Deswegen müssen Sie die VDDK-Setup-Dateien nicht von der VMware-Website herunterladen, um CA ARCserve D2D auf Remote-Knoten bereitzustellen.

Installieren von CA ARCserve Central Protection Manager

Der Installationsassistent hilft Ihnen dabei, führt Sie durch den Prozess, CA ARCserve Central Applications einmal oder mehrmals zu installieren.

Hinweis: Bevor Sie die Anwendung installieren, überprüfen Sie die Datei mit den Versionshinweisen und stellen Sie sicher, dass alle in Vorbereitende Aufgaben beschriebene Aufgaben ausgeführt sind.

So installieren Sie CA ARCserve Central Protection Manager

1. Laden Sie das CA ARCserve Central Applications-Installationspaket auf den Computer herunter, auf dem Sie die Anwendung installieren möchten, und doppelklicken Sie dann auf die Setup-Datei.

   Das Installationspaket extrahiert seine Inhalte auf Ihren Computer und daraufhin öffnet sich das Dialogfeld "Erforderliche Komponenten".

2. Klicken Sie im Dialogfeld "Erforderliche Komponenten" auf "Installieren".

   Hinweis: Das Dialogfeld "Erforderliche Komponenten" wird nur angezeigt, wenn Setup die erforderlichen Komponenten nicht auf dem Zielcomputer installiert findet.

   Nachdem Setup die erforderlichen Komponenten installiert hat, öffnet sich das Dialogfeld "Lizenzvereinbarung".

3. Füllen Sie die erforderlichen Optionen auf der Lizenzvereinbarung aus, und klicken Sie auf "Weiter".

   Das Dialogfeld "Konfiguration" wird geöffnet.

4. Führen Sie auf dem Dialogfeld "Konfiguration" folgende Schritte aus:

   - **Komponenten**: Geben Sie die Anwendungen an, die Sie installieren wollen.

     Hinweis: Wenn Sie diese Anwendung mithilfe des Suite-Installationspakets installieren, können Sie mehrere Anwendungen installieren.

   - **Speicherort**: Akzeptieren Sie den Standardspeicherort für die Installation oder klicken Sie auf "Durchsuchen", um einen alternativen Installationsspeicherort anzugeben. Der Standardspeicherort lautet folgendermaßen:

     ```
     C:\Programme\CA\ARCserve Central Applications
     ```

   - **Festplatteninformationen**: Stellen Sie sicher, dass Ihre Festplatte über ausreichenden Speicherplatz verfügt, um die Anwendungen zu installieren.

   - **Name des Windows-Administrators**: Geben Sie den Benutzernamen des Windows-Administratorkontos unter Verwendung der folgenden Syntax an:

     ```
     Domäne\Benutzername
     ```

   - **Kennwort:** Geben Sie das Kennwort für das Benutzerkonto an.

   - **Portnummer angeben:** Geben Sie die Portnummer an, die Sie verwenden wollen, um mit der webbasierten Benutzeroberfläche zu kommunizieren. Als Best Practice sollten Sie die standardmäßige Portnummer akzeptieren. Die standardmäßige Portnummer lautet:

     ```
     8015
     ```

     Hinweis: Wenn Sie eine alternative Portnummer angeben wollen, liegen die verfügbaren Portnummern zwischen 1024 und 65535. Bevor Sie eine alternative Portnummer angeben, überprüfen Sie, ob die festgelegte Portnummer frei und zur Verwendung verfügbar ist. Setup hindert Sie daran, die Anwendung mithilfe eines Ports zu installieren, der nicht zur Verwendung verfügbar ist.

- **Für Web-Kommunikationen HTTPS verwenden:** Legen Sie die Verwendung der HTTPS-Kommunikation für Datenübertragung fest. Standardmäßig ist diese Option deaktiviert.

  Hinweis: Sichere HTTPS-Kommunikation bietet eine höhere Sicherheitsebene als HTTP-Kommunikation. HTTPS ist das empfohlene Kommunikationsprotokoll, wenn Sie in Ihrem Netzwerk vertrauliche Informationen übertragen.

- **Lassen Sie zu, dass Setup die Dienste und Programme von CA ARCserve Central Applications als Ausnahmen für die Windows Firewall registriert --**Stellen Sie sicher, dass das Kontrollkästchen neben dieser Option aktiviert ist. Firewall-Ausnahmen sind erforderlich, wenn Sie CA ARCserve Central Applications von Remote-Rechnern aus konfigurieren und verwalten möchten.

  Hinweis: Benutzer, die die Anwendung lokal verwenden, brauchen keine Firewall-Ausnahmen zu registrieren.

Klicken Sie auf "Weiter".

Das Dialogfeld "Datenbankeinstellungen" wird geöffnet.

5. Klicken Sie im Dialogfeld "Datenbankeinstellungen" auf die Drop-down-Liste neben "Wählen Sie den Datenbanktyp aus" und aktivieren Sie eine der folgenden Optionen.

   - ARCserve Central Applications-Standarddatenbank
   - Microsoft SQL Server

   Nachdem Sie einen Datenbanktyp angegeben haben, werden die erforderlichen Optionen für die angegebene Datenbank im Dialogfeld "Datenbankeinstellungen" angezeigt.

6. Wählen Sie eine der folgenden Vorgehensweisen:

   - **ARCserve Central Applications-Standarddatenbank:** Füllen Sie die folgenden Felder im Dialogfeld "Datenbankeinstellungen" aus:

     - **Installationspfad festlegen:** Geben Sie den Speicherort an, wo Sie die CA ARCserve Central Applications-Standarddatenbank installieren möchten. Sie können den Standardpfad übernehmen oder einen anderen Pfad angeben.
     - **Datendateipfad festlegen:** Geben Sie den Speicherort an, an dem Sie die Datendatei für die CA ARCserve Central Applications-Standarddatenbank installieren möchten. Sie können den Standardpfad übernehmen oder einen anderen Pfad angeben.

     Hinweis: Die CA ARCserve Central Applications-Standarddatenbank unterstützt keine Remote-Kommunikation. Installieren Sie daher die Standarddatenbank und die Datendatei auf dem Computer, auf dem Sie die Anwendung installieren.

- **Microsoft SQL Server-Datenbank:** Füllen Sie die folgenden Felder im Dialogfeld "Datenbankeinstellungen" aus:
  - **SQL Server-Typ:** Geben Sie die Kommunikationsart an, die die Anwendung verwenden soll, um mit der SQL Server-Datenbank zu kommunizieren.

    Lokal: Geben Sie "Lokal" an, wenn die Anwendung und SQL Server auf dem gleichen Computer installiert sind.

    Remote: Geben Sie "Remote" an, wenn die Anwendung und SQL Server auf unterschiedlichen Computern installiert sind.
  - **SQL Server-Name**: Wenn der angegebene SQL Server-Typ "Remote" ist, geben Sie den Namen des Remote-SQL-Servers an. Wenn der SQL-Server lokal verwendet wird, wählen Sie den Server aus der Drop-down-Liste aus.
  - **Sicherheit:** Geben Sie den Typ der Anmeldeinformationen an, mit denen Sie die SQL Server-Authentifizierung abwickeln möchten.

    Windows-Sicherheit verwenden: Geben Sie "Windows-Sicherheit verwenden" an, um die Authentifizierung mit Ihren Windows-Anmeldeinformationen abzuwickeln.

    SQL Server-Sicherheit verwenden: Geben Sie "SQL Server-Sicherheit verwenden" an, um die Authentifizierung mit Ihren SQL Server-Anmeldeinformationen abzuwickeln. Geben Sie anschließend die Anmelde-ID und das Kennwort für das SQL Server-Konto an.
  - **Vorhandene Datenbank überschreiben:** Geben Sie "Vorhandene Datenbank überschreiben" an, wenn Setup die vorhandene CA ARCserve Central Applications-Datenbank erkennen und überschreiben soll.

  Klicken Sie auf "Installieren".

  Nachdem der Installationsprozess abgeschlossen ist, öffnet sich das Dialogfeld "Installationsbericht".

7. Das Dialogfeld "Installationsbericht" fasst die Installation zusammen. Wenn Sie jetzt nach Aktualisierungen für die Anwendung suchen wollen, klicken Sie auf "Nach Aktualisierungen suchen" und danach auf "Fertig stellen".

Die Anwendung wird installiert.

CA ARCserve Central Protection Manager automatisch installieren

CA ARCserve Central Applications lässt Sie CA ARCserve Central Protection Manager automatisch installieren. Bei der automatischen Installation ist kein Benutzereingriff erforderlich. Die folgenden Schritte beschreiben, wie Sie die Anwendung mithilfe der Windows-Befehlszeile automatisch installieren können.

So installieren Sie CA ARCserve Central Protection Manager automatisch

1. Öffnen Sie die Windows-Befehlszeile auf dem Computer, auf dem Sie den automatischen Installationsvorgang starten wollen.
2. Laden Sie das selbstextrahierende
   CA ARCserve Central Applications-Installationspaket auf Ihren Computer herunter.

   Starten Sie den automatischen Installationsvorgang mithilfe der folgenden Befehlszeilen-Syntax:

   ```
   "CA ARCserve Central Applications Setup.exe" /s /v"/q
   -Path:<INSTALLATIONSVERZEICHNIS> -Port:<PORT> -U:<Benutzername> -P:<Kennwort>
   -Products:<Produktliste>"
   ```

   Verwendung:

   s

   Lässt Sie das ausführbare Dateipaket im automatischen Modus ausführen.

   v

   Lässt Sie zusätzliche Befehlszeilenoptionen angeben.

   q

   Lässt Sie die Anwendung im automatischen Modus installieren.

   -Path:<INSTALLATIONSVERZEICHNIS>

   (Optional) Lässt Sie den Zielinstallationspfad festlegen.

   Beispiel:

   ```
   -Path:“C:\Programme\CA\ARCserve Central Applications”
   ```

   Hinweis: Wenn der Wert für INSTALLATIONSVERZEICHNIS ein Leerzeichen enthält, setzen Sie den Pfad zwischen umgekehrte Schrägstriche und Anführungszeichen. Zudem kann der Pfad nicht mit einem umgekehrten Schrägstrich enden.

   -Port:<PORT>

   (Optional) Lässt Sie die Portnummer für die Kommunikation festlegen.

   Beispiel:

   ```
   -Port:8015
   ```

-U:<Benutzername>

Lässt Sie den Benutzernamen festlegen, der verwendet werden soll, um die Anwendung zu installieren und auszuführen.

Hinweis: Der Benutzername muss ein Administratorkonto oder ein Konto mit Administratorrechten sein.

-P:<Kennwort>

Lässt Sie das Kennwort für den Benutzernamen festlegen.

-Products:<ProductList>

(Optional) Ermöglicht es Ihnen, die CA ARCserve Central Applications-Anwendungen anzugeben, die automatisch installiert werden sollen. Wenn Sie keinen Wert für dieses Argument angeben, installiert der automatische Installationsvorgang alle Komponenten der CA ARCserve Central Applications-Anwendungen.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

Alle CA ARCserve Central Applications

ALLE

Hinweis: Die folgenden Beispiele beschreiben die Syntax, die erforderlich ist, um eine, zwei, drei oder alle CA ARCserve Central Applications automatisch zu installieren:

```
-Products:CMX64
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:ALL
```

Die Anwendung wird automatisch installiert.

So deinstallieren Sie CA ARCserve Central Protection Manager.

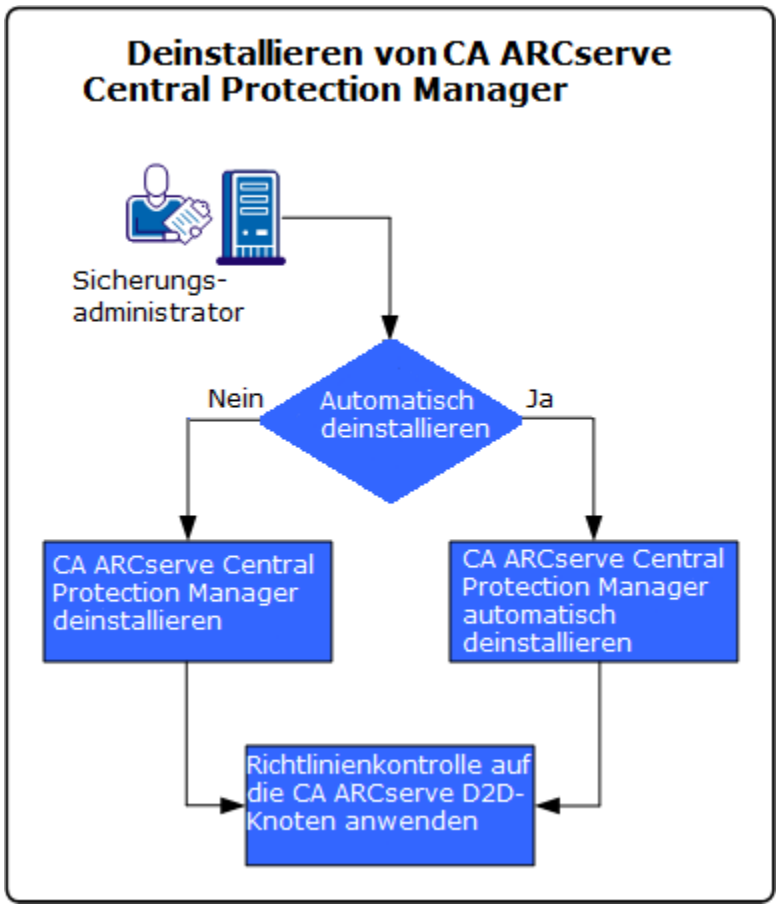
Sie können CA ARCserve Central Protection Manager folgendermaßen deinstallieren:

- Standardmäßige Deinstallation: Diese Methode verwendet die Windows-Systemsteuerung, um die Anwendung zu deinstallieren.
- Automatische Deinstallation: Diese Methode lässt Sie eine unbeaufsichtigte Deinstallation unter Verwendung der Windows-Befehlszeile ausführen.

Richtlinienzuweisungen aufheben

Als Best Practice empfiehlt es sich, die Zuweisung aller Richtlinien zu den Knoten aufzuheben, denen sie zugewiesen sind, bevor Sie die Anwendung deinstallieren. Wir empfehlen diese Vorgehensweise, weil Sie keine CA ARCserve D2D-Sicherungseinstellungen auf dem Knoten festlegen können, solange einem Knoten eine CA ARCserve Central Protection Manager-Richtlinie zugewiesen ist. Außerdem können Sie Zuweisungen von Richtlinien zu Knoten nicht mehr aufheben, nachdem Sie die Anwendung deinstalliert haben. CA ARCserve D2D stellt ein Befehlszeilenhilfsprogramm zur Verfügung, mit dem Sie Zuweisungen von Richtlinien zu Knoten aufheben können, nachdem Sie die Anwendung deinstalliert haben.

Das folgende Diagramm veranschaulicht, wie Sie die Anwendung deinstallieren:


Deinstallieren von CA ARCserve Central Protection Manager
Sicherungs-administrator
Automatisch deinstallieren
Nein
Ja
CA ARCserve Central Protection Manager deinstallieren
CA ARCserve Central Protection Manager automatisch deinstallieren
Richtlinienkontrolle auf die CA ARCserve D2D-Knoten anwenden

Aufgabe	Siehe Thema
Führen Sie eine standardmäßige Deinstallation mithilfe der Windows-Systemsteuerung aus.	CA ARCserve Central Protection Manager deinstallieren (siehe Seite 25)
Führen Sie eine automatische Deinstallation mithilfe der Windows-Befehlszeile aus.	CA ARCserve Central Protection Manager automatisch deinstallieren (siehe Seite 26)
Heben Sie die Zuweisung von Richtlinien zu Knoten auf, nachdem Sie CA ARCserve Central Protection Manager deinstalliert haben.	Richtlinienkontrolle auf die CA ARCserve D2D-Knoten anwenden (siehe Seite 27).

Deinstallieren von CA ARCserve Central Protection Manager

Sie können CA ARCserve Central Protection Manager mithilfe von Programmen und in der Windows-Systemsteuerung befindlichen Funktionen deinstallieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, von dem Sie die Anwendung deinstallieren möchten.

   Hinweis: Sie müssen sich über ein administratives Konto oder ein Konto mit administrativen Berechtigungen anmelden.

2. Klicken Sie im Windows-Startmenü auf "Start" und auf "Systemsteuerung", um die Windows-Systemsteuerung zu öffnen.

3. Klicken Sie auf "Programme und Funktionen", um das Fenster "Programm deinstallieren oder ändern" zu öffnen.

4. Suchen Sie CA ARCserve Central Protection Manager und klicken Sie darauf.

   Klicken Sie mit der rechten Maustaste auf die Anwendung und im Pop-up-Menü auf "Deinstallieren".

   Folgen Sie den Bildschirmanweisungen, um die Anwendung zu deinstallieren.

Die Anwendung wird deinstalliert.

CA ARCserve Central Protection Manager automatisch deinstallieren

CA ARCserve Central Applications lässt Sie CA ARCserve Central Protection Manager automatisch deinstallieren. Bei der automatischen Installation ist kein Benutzereingriff erforderlich. Die folgenden Schritte beschreiben, wie Sie die Anwendung mithilfe der Windows-Befehlszeile automatisch deinstallieren können.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Computer an, von dem Sie die Anwendung deinstallieren möchten.

   Hinweis: Sie müssen sich über ein administratives Konto oder ein Konto mit administrativen Berechtigungen anmelden.

2. Öffnen Sie die Windows-Befehlszeile, und führen Sie folgenden Befehl aus, um den automatischen Deinstallationsvorgang zu starten:

   ```
   <INSTALLATIONSVERZEICHNIS>%\Setup\uninstall.exe /q /p <Produktcode>
   ```

   Oder

   ```
   <INSTALLATIONSVERZEICHNIS>%\Setup\uninstall.exe /q /ALL
   ```

   Beispiel: Mit der folgenden Syntax können Sie die Anwendung automatisch deinstallieren.

   ```
   "%Programme%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED05FE-D895-4FD5-B964-001928BD2D62}
   ```

   Verwendung:

   <INSTALLATIONSVERZEICHNIS>

   Hier können Sie das Verzeichnis angeben, in dem die Anwendung installiert ist.

   Hinweis: Führen Sie die Syntax aus, die der Architektur des Betriebssystems des Computers entspricht.

   <Produktcode>

   Hier können Sie die Anwendung angeben, die automatisch deinstalliert werden soll. Verwenden Sie die folgenden Produktcodes, um
   CA ARCserve Central Applications automatisch zu deinstallieren.

   CA ARCserve Central Protection Manager

   ```
   {CAED05FE-D895-4FD5-B964-001928BD2D62}
   ```

   CA ARCserve Central Host-Based VM Backup

   ```
   {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}
   ```

   CA ARCserve Central Reporting

   ```
   {CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}
   ```

   CA ARCserve Central Virtual Standby

   ```
   {CAED4835-964B-484B-A395-E2DF12E6F73D}
   ```

Die Anwendung wird automatisch deinstalliert.

Richtlinienkontrolle auf die CA ARCserve D2D-Knoten anwenden

Durch die Deinstallation von CA ARCserve Central Protection Manager wird die Zuweisung die Sicherungsrichtlinien zu den CA ARCserve D2D-Knoten nicht aufgehoben. Dadurch können Sie Sicherungseinstellungen nicht direkt auf den CA ARCserve D2D-Knoten festlegen, nachdem Sie Protection Manager deinstalliert haben. Als Best Practice empfiehlt es sich, die Zuweisung aller Richtlinien zu den Knoten aufzuheben, denen sie zugewiesen sind, bevor Sie die Anwendung deinstallieren. Wenn Sie diese Methode nicht ausführen, können Sie die Richtlinienkontrolle mithilfe eines speziell dazu entworfenen Hilfsprogramms auf die Knoten anwenden.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim CA ARCserve D2D-Knoten an.
2. Öffnen Sie die Windows-Befehlszeile, und wechseln Sie in das folgende Verzeichnis:

   ```
   C:\Programme\CA\ARCserve D2D\BIN
   ```

3. Führen Sie die Datei "ARCCentralAppMgrUtility.exe" unter Verwendung folgender Syntax aus:

   ```
   ARCCentralAppMgrUtility.exe -clean pm|hbvb|vs [-debug]
   ```

   pm|hbvb|vs

   Definiert die Anwendung, für die Sie die Kontrolle des CA ARCserve D2D-Knotens aufheben wollen. Wählen Sie eines der folgenden Argumente:

   pm

   CA ARCserve Central Protection Manager

   hbvb

   CA ARCserve Central Host-Based VM Backup

   vs

   CA ARCserve Central Virtual Standby

   -debug

Die Option "-debug" ist nicht erforderlich. Wenn diese Option aktiviert ist, generiert das Hilfsprogramm eine Debug-Protokolldatei, die im folgenden Verzeichnis gespeichert wird:

```
<D2D_Home>\Log\ARCCentralAppMgrUtility.log
```

Beispiel: Das folgende Beispiel beschreibt die Syntax für das Anwenden der Richtlinienkontrolle auf den Knoten.

```
ARCCentralAppMgrUtility.exe -clean pm
```

Die Richtlinienkontrolle wird auf den Knoten angewendet.

Auswirkungen des Installationsprozesses auf das Betriebssystem

Durch den CA ARCserve Central Applications-Installationsprozess werden mithilfe des Installationsmoduls "Microsoft-Installationspaket" (MSI) verschiedene Komponenten des Windows-Betriebssystems aktualisiert. Mit den im MSI enthaltenen Komponenten kann CA ARCserve Central Applications benutzerdefinierte Aktionen zum Installieren, Aktualisieren oder Deinstallieren von CA ARCserve Central Applications durchführen.

In der folgenden Liste sind die benutzerdefinierten Aktionen und die betroffenen Komponenten aufgeführt.

Hinweis: Alle CA ARCserve Central Applications-MSI-Pakete rufen die in dieser Tabelle enthaltenen Komponenten auf, wenn Sie CA ARCserve Central Applications installieren und deinstallieren.

Komponente	Beschreibung
CallAllowInstall	Hiermit werden beim Installationsvorgang die Bedingungen überprüft, die einen Bezug zur aktuellen CA ARCserve Central Applications-Installation haben.
CallPreInstall	Hiermit können beim Installationsprozess MSI-Eigenschaften gelesen und geschrieben werden. Beispielsweise kann der CA ARCserve Central Applications-Installationspfad im MSI gelesen werden.
CallPostInstall	Hiermit können beim Installationsprozess verschiedene mit der Installation verbundene Aufgaben ausgeführt werden. Beispielsweise kann CA ARCserve Central Applications in der Windows-Registrierung registriert werden.
CallAllowUninstall	Hiermit werden beim Deinstallationsvorgang die Bedingungen überprüft, die einen Bezug zur aktuellen CA ARCserve Central Applications-Installation haben.

Komponente	Beschreibung
CallPreUninstall	Hiermit können beim Deinstallationsprozess verschiedene mit der Installation verbundene Aufgaben ausgeführt werden. Beispielsweise kann die Registrierung von CA ARCserve Central Applications in der Windows-Registrierung rückgängig gemacht werden.
CallPostUninstall	Hiermit werden beim Deinstallationsvorgang mehrere Aufgaben ausgeführt, nachdem die installierten Dateien deinstalliert wurden. Zum Beispiel können die restlichen Dateien entfernt werden.
ShowMsiLog	Zeigt die Protokolldatei von Windows Installer in Notepad an, wenn der Endbenutzer in den Dialogfeldern "Setup erfolgreich", "Setup fehlgeschlagen" oder "Setup unterbrochen" das Kontrollkästchen der Option "Protokolldatei von Windows Installer anzeigen" aktiviert und dann auf "Fertig stellen" klickt. (Dies funktioniert lediglich mit Windows Installer 4.0.)
ISPrint	Druckt die Inhalte eines Steuerelements mit scrollbarem Text auf einem Dialogfeld aus. Dies ist eine benutzerdefinierte Aktion der Windows-Installer-DLL. Die DLL-Datei heißt SetAllUsers.dll, und ihre Einsprungstelle ist PrintScrollableText.
CheckForProductUpdates	Verwendet FLEXnet Connect, um auf Produktaktualisierungen zu prüfen. Diese benutzerdefinierte Aktion startet eine ausführbare Datei mit dem Namen "Agent.exe" und gibt folgende Informationen weiter: /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Verwendet FLEXnet Connect, um nach dem Neustart auf Produktaktualisierungen zu prüfen. Diese benutzerdefinierte Aktion startet eine ausführbare Datei mit dem Namen "Agent.exe" und gibt folgende Informationen weiter: /au[ProductCode] /EndOfInstall /Reboot

- **Aktualisierte Verzeichnisse:** Während des Installationsvorgangs werden CA ARCserve Central Applications-Dateien standardmäßig in den folgenden Verzeichnissen installiert und aktualisiert:

  `C:\Programme\CA\ARCserve Central Applications`

  Sie können CA ARCserve Central Applications im Standardinstallationsverzeichnis oder in einem alternativen Installationsverzeichnis installieren. Der Installationsprozess kopiert verschiedene Systemdateien ins folgende Verzeichnis:

  `C:\WINDOWS\SYSTEM32`

- **Aktualisierte Windows-Registrierungsschlüssel:** Der Installationsprozess aktualisiert die folgenden Windows-Registrierungsschlüssel:

  Standard-Registrierungsschlüssel:

  `HKLM\SOFTWARE\CA\CA ARCserve Central Applications`

  Basierend auf der aktuellen Konfiguration Ihres Systems werden beim Installationsprozess neue Registrierungsschlüssel erstellt und verschiedene weitere Registrierungsschlüssel geändert.

- **Installierte Anwendungen:** Beim Installationsprozess werden folgende Anwendungen auf Ihrem Computer installiert:
  - CA Licensing
  - Microsoft Visual C++ 2005 SP1 Redistributable
  - Microsoft Windows Installer 3.1 Redistributable (v2) Package
  - Java Runtime Environment (JRE) 1.6.0_16
  - Tomcat 6.0.32

Binärdateien mit unrichtigen Informationen zur Dateiversion

CA ARCserve Central Applications installiert Binärdaten von Drittanbietern, aus anderen CA-Produkten und aus CA ARCserve Central Applications, die unrichtige Informationen zur Dateiversion enthalten. In der folgenden Tabelle werden diese Binärdaten beschrieben.

Binärname	Quelle
UpdateData.exe	CA License
zlib1.dll	Zlib Compression Library

Binärdateien ohne eingebettetes Manifest

CA ARCserve Central Applications installiert Binärdaten von Drittanbietern, aus anderen CA Technologies-Produkten und aus CA ARCserve Central Applications, die kein eingebettetes Manifest und kein Text-Manifest enthalten. In der folgenden Tabelle werden diese Binärdaten beschrieben.

Binärname	Quelle
BaseLicInst.exe	CA License
UpdateData.exe	CA License

Binärname	Quelle
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
tomcat6.exe	Tomcat

Binärdateien mit "Require Administrator"-Berechtigungen im Manifest

CA ARCserve Central Applications installiert Binärdaten von Drittanbietern, aus anderen CA Technologies-Produkten und aus CA ARCserve Central Applications, die über die Berechtigungsebene "Administrator" oder "Highest Available" verfügen. Sie müssen sich mit einem Administratorkonto oder einem Konto mit den höchstmöglichen Berechtigungen anmelden, um verschiedene Dienste, Komponenten und Anwendungen von CA ARCserve Central Applications ausführen zu können. Die Binärdateien für diese Dienste, Komponenten und Anwendungen enthalten
CA ARCserve Central Applications-spezifische Funktionen, die für ein normales Benutzerkonto nicht verfügbar sind. Daher werden Sie von Windows aufgefordert, einen Vorgang zu bestätigen, indem Sie Ihr Kennwort angeben oder ein Konto mit Administratorrechten verwenden, um den Vorgang auszuführen.

- **Administratorrechte** - Das Administratorprofil sowie Konten mit Administratorrechten verfügen über Schreib-, Lese- und Ausführungsberechtigungen für alle Windows- und Systemressourcen. Wenn Sie über keine Administratorrechte verfügen, werden Sie aufgefordert, den Benutzernamen und das Kennwort eines Administrators einzugeben, um fortfahren zu können.
- **Höchstmögliche Berechtigungen** - Bei einem Konto mit den höchst möglichen Berechtigungen handelt es sich um ein normales Benutzerkonto oder Poweruser-Konto, mit dem Administratorrechte genutzt werden können.

In der folgenden Tabelle werden diese Binärdaten beschrieben.

Binärname	Quelle
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications

Binärname	Quelle
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Kapitel 3: Erste Schritte mit CA ARCserve Central Protection Manager

Folgende Abschnitte beschreiben, wie CA ARCserve Central Protection Manager konfiguriert werde sollte, um CA ARCserve D2D-Knoten zu schützen.

Dieses Kapitel enthält folgende Themen:

Sicherstellen, dass der CA ARCserve Central Protection Manager-Server mit den Knoten kommunizieren kann (siehe Seite 34)
Konfigurieren von CA ARCserve Backup-Datensynchronisations-Ablaufplänen (siehe Seite 34)
Konfigurieren von SRM-Ablaufplänen (siehe Seite 35)
Konfigurieren von Discovery-Ablaufplänen (siehe Seite 36)
Konfigurieren von E-Mail- und Alert-Einstellungen (siehe Seite 36)
Konfigurieren der Einstellungen von IT-Verwaltungsservern (siehe Seite 38)
Konfigurieren von Ablaufplänen für Aktualisierungen von CA ARCserve Central Applications (siehe Seite 39)
Konfigurieren von Voreinstellungen für Social Networking (siehe Seite 41)
Ändern des Administratorkontos (siehe Seite 42)
Konfigurieren der Einstellungen für die Bereitstellung von D2D (siehe Seite 43)
Konfigurieren der Datenbank (siehe Seite 44)
CA ARCserve Central Protection Manager-Datenbank erneut erstellen (siehe Seite 45)

Sicherstellen, dass der CA ARCserve Central Protection Manager-Server mit den Knoten kommunizieren kann

Hinweis: Dies ist ein optionaler Schritt dazu, CA ARCserve Central Protection Manager so zu konfigurieren, dass es Knoten schützt.

Um sicherzustellen, dass CA ARCserve Central Protection Manager Richtlinien auf Knoten bereitstellen und Knoten schützen kann, müssen Sie überprüfen, ob der Protection Manager-Server und die Knoten, die Sie schützen wollen, mithilfe ihrer Hostnamen miteinander kommunizieren können.

So stellen Sie sicher, dass der CA ARCserve Central Protection Manager-Server mit den Knoten kommunizieren kann:

1. Pingen Sie vom CA ARCserve Central Protection Manager-Server aus mit den Hostnamen der Knoten die Knoten an, die Sie schützen wollen.
2. Pingen Sie von den Knoten aus, die Sie schützen wollen, den CA ARCserve Central Protection Manager-Server mit dem Hostnamen des Servers an.

Konfigurieren von CA ARCserve Backup-Datensynchronisations-Ablaufplänen

Die CA ARCserve Backup-Datensynchronisation ermöglicht es Ihnen, das System so zu konfigurieren, dass eine geplante Zeit und Wiederholungsmethode festgelegt wird, die bestimmt, an wie vielen Tagen und an welchem Tag der Woche oder des Monats der Benutzer die CA ARCserve Backup-Datenbank mit der CA ARCserve Central Protection Manager-Datenbank synchronisieren kann.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.
2. Klicken Sie in der Navigationsleiste auf "Konfiguration", um die Ansicht "Konfiguration" zu öffnen.
3. Klicken Sie im Feld "Konfiguration" auf "Ablaufplan der CA ARCserve Backup-Datensynchronisation", um die Optionen der CA ARCserve Backup-Datensynchronisation anzuzeigen.
4. Klicken Sie auf "Aktivieren", um die CA ARCserve Backup-Datensynchronisation zu aktivieren.

   Hinweis: Standardmäßig ist die Konfiguration der CA ARCserve Backup-Datensynchronisation aktiviert.

5. Geben Sie die folgenden Parameter an, um die CA ARCserve Backup-Datensynchronisation zu planen:
   - Wiederholungsmethode
   - Geplante Zeit
6. Klicken Sie auf "Speichern", um den Ablaufplan der CA ARCserve Backup-Datensynchronisation anzuwenden.
7. (Optional) Klicken Sie auf "Jetzt ausführen", um den CA ARCserve Backup-Datensynchronisationsprozess zu starten.

Konfigurieren von SRM-Ablaufplänen

CA ARCserve Central Protection Manager lässt Sicherungsadministratoren einen Ablaufplan für CA ARCserve D2D-Knoten konfigurieren, der festlegt, wann und wie oft SRM-Daten erfasst werden. SRM (Speicherressourcenverwaltung) ist eine Funktionalität, die Informationen über das Folgende erfasst:

- Hardware, Software und Anwendungsdaten für Microsoft SQL Server- und Microsoft Exchange Server-Implementierungen.
- Leistungskennzahldaten (PKI) von CA ARCserve D2D-Servern, die von einem CA ARCserve Central Applications-Server verwaltet werden.

  Hinweis: Für CA ARCserve Backup-Knoten erfasst CA ARCserve Backup PKI-Daten und synchronisiert die Daten daraufhin während des CA ARCserve Backup-Datensynchronisationsprozesses mit CA ARCserve Central Protection Manager.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.
2. Öffnen Sie die Ansicht "Konfiguration" durch Klicken auf "Konfiguration" in der Navigationsleiste.
3. Klicken Sie im Feld "Konfiguration" auf "SRM-Konfiguration", um die Optionen der SRM-Konfiguration anzuzeigen.
4. Klicken Sie auf "Aktivieren", um SRM zu aktivieren.

   Hinweis: Standardmäßig ist die SRM-Konfiguration aktiviert.
5. Geben Sie die folgenden Parameter an, um SRM zu planen:
   - Wiederholungsmethode
   - Geplante Zeit
6. Klicken Sie auf "Speichern", um den SRM-Ablaufplan anzuwenden.
7. (Optional) Klicken Sie auf "Jetzt ausführen", um den SRM-Datenerfassungsprozess zu starten.

Konfigurieren von Discovery-Ablaufplänen

Für den Discovery-Ablaufplan für Knoten können Sie einen bestimmten Zeitpunkt und das Wiederholungsintervall konfigurieren. Standardmäßig ist "Discovery-Konfiguration" deaktiviert. Um die Konfiguration zu aktivieren, klicken Sie auf die Option "Aktivieren", um die von Ihnen gewünschte Wiederholungsmethode und einen bestimmten Zeitpunkt für den Beginn der Knoten-Discovery festzulegen. Sie können die folgenden Parameter festlegen, um Ihren Discovery-Ablaufplan zu konfigurieren:

- **Nach folgender Anzahl von Tagen:** Lässt Sie die Methode nach der angegebenen Anzahl von Tagen wiederholen. (Standard)
- **Alle ausgewählten Tage der Woche:** Lässt Sie die Methode an den angegebenen Tagen wiederholen. Montag, Dienstag, Mittwoch, Donnerstag und Freitag sind die standardmäßigen Wochentage.
- **Alle ausgewählten Tage des Monats:** Lässt Sie die Methode am angegebenen Tag des Monats wiederholen. 1 ist die Standardoption für den Tag des Monats.

Eine Active Directory-Liste wird für Sie angezeigt, wenn Sie einen Ablaufplan zur Erkennung von Knoten einrichten.

Konfigurieren von E-Mail- und Alert-Einstellungen

Sie können die E-Mail- und Alert-Einstellungen für die Verwendung mit Ihrer Anwendung konfigurieren, um gemäß der Bedingungen, die Sie angeben, automatische Warnmeldungen zu versenden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste der Startseite auf "Konfiguration" um die Ansicht "Konfiguration" zu öffnen.

2. Klicken Sie vom Konfigurationsbereich auf "E-Mail- und Alert-Konfiguration", um die E-Mail- und Alert-Konfigurationsoptionen zu öffnen.

3. Füllen Sie die folgenden Felder aus:

   - **Dienst**: Geben Sie im Drop-down-Feld den Typ des E-Mail-Dienstes. (Google Mail, Yahoo Mail, Live Mail oder andere)
   - **E-Mail-Server**: Geben Sie den Hostnamen des SMTP-Servers an, den CA ARCserve Central Applications verwenden soll, um E-Mails zu senden.
   - **Erfordert Authentifizierung**: Wählen Sie diese Option aus, wenn der angegebene E-Mail-Server, Authentifizierung benötigt. Der Kontoname und das Kennwort müssen angegeben werden.
   - **Betreff**: Geben Sie einen standardmäßigen E-Mail-Betreff an.
   - **Von**: Geben Sie die E-Mail-Adresse an, von der die E-Mail geschickt wird.
   - **Empfänger**: Geben Sie eine oder mehrere durch Semikolon (;) getrennte E-Mail-Adressen an, an die die E-Mail geschickt wird.
   - **SSL verwenden**: Wählen Sie diese Option aus, wenn der angegebene E-Mail-Server eine sichere Verbindung (SSL) erfordert.
   - **STARTTLS senden**: Wählen Sie diese Option aus, wenn der angegebene E-Mail-Server einen STARTTLS-Befehl erfordert.
   - **HTML-Format verwenden**: Ermöglicht es Ihnen, die E-Mails in HTML-Format zu senden. (Standardmäßig ausgewählt)
   - **Proxy-Einstellungen aktivieren**: Wählen Sie diese Option aus, wenn ein Proxy-Server vorhanden ist, und geben Sie anschließend die Proxy-Server-Einstellungen an.

4. Klicken Sie auf "Test-E-Mail", um zu sicherzustellen, dass die E-Mail-Konfigurationseinstellungen richtig sind.

5. (Optional) Klicken Sie im Bereich "E-Mail-Alerts senden" auf "Erkannte Knoten", um die Anwendung E-Mail-Warnungs-Meldungen senden zu lassen, wenn neue Knoten entdeckt werden.

6. Klicken Sie auf "Speichern".

   Hinweis: Sie können auf "Zurücksetzen" klicken, um zu den früher gespeicherten Werten zurückzukehren, oder auf "Löschen", um Ihre gespeicherten Einstellungen zu löschen. Das Löschen Ihrer E-Mail- und Alert-Einstellungen hat zur Folge, dass Sie keine E-Mail-Warnungs-Meldungen empfangen.

Die E-Mail-Konfiguration wird angewendet.

Konfigurieren der Einstellungen von IT-Verwaltungsservern

Mit CA ARCserve Central Protection Manager können Sie Alert-Meldungen an IT-Verwaltungsserver senden. Um die Alert-Informationen zu senden, konfigurieren Sie den Anwendungsserver für die Kommunikation mit dem IT-Verwaltungsserver.

So konfigurieren Sie die Einstellungen von IT-Verwaltungsservern

1. Melden Sie sich beim CA ARCserve Central Protection Manager an und klicken Sie in der Navigationsleiste auf "Konfiguration".
2. Klicken Sie im Bildschirm "Konfiguration" auf die Konfiguration des IT-Verwaltungsservers in der Konfigurationsliste.
3. Vervollständigen Sie folgende Konfigurationsoptionen für den IT-Verwaltungsserver:
   - Klicken Sie auf "Aktivieren".
   - Klicken Sie auf "Nimsoft" oder "Kasaya".
   - Geben Sie eine Wiederholungsmethode an. Die Wiederholungsmethode legt die Wochentage fest, an denen Alert-Benachrichtigungen zurück an den IT-Verwaltungsserver gesendet werden sollen, wenn der ursprüngliche Sendeprozess fehlgeschlagen ist. Der Alert-Sendeprozess kann fehlschlagen, wenn der IT-Verwaltungsserver nicht verfügbar oder offline ist.
   - Geben Sie einen Ablaufplan an. Der Ablaufplan legt die Zeit des Tages fest, an dem die Alert-Benachrichtigungen an den Nimsoft-Server zurück gesendet werden sollen.
4. Klicken Sie auf "Speichern".

Der CA ARCserve Central Protection Manager-Server ist so konfiguriert, dass er mit dem IT-Verwaltungsserver kommuniziert.

Hinweis: Sie können auf "Zurücksetzen" klicken, um zu den zuvor gespeicherten Werten zurückzukehren.

Konfigurieren von Ablaufplänen für Aktualisierungen von CA ARCserve Central Applications

Mit der Anwendung können Sie einen Ablaufplan einrichten, der automatisch Produktaktualisierungen von einem CA-Server oder einem lokalen Software-Staging-Server herunterlädt.

So konfigurieren Sie Ablaufpläne für automatische Aktualisierungen von CA ARCserve Central Applications

1. Melden Sie sich bei der Anwendung an.
2. Klicken Sie in der Navigationsleiste auf "Konfiguration", um die Ansicht "Konfiguration" zu öffnen.
3. Klicken Sie im Konfigurationsbereich auf "Konfiguration aktualisieren".

   Die Optionen für die Aktualisierung der Konfiguration werden angezeigt.
4. Wählen Sie einen Download-Server aus.
   - **CA-Server:** Klicken Sie für folgende Optionen auf "Proxy-Einstellungen":
     - **Proxy-Einstellungen des Browsers verwenden:** Lässt Sie die Anmeldeinformationen verwenden, die für die Proxy-Einstellungen des Browsers vorbereitet wurden.

       Hinweis: Die Option "Proxy-Einstellungen des Browsers verwenden" wirkt sich auf Internet Explorer und Chrome aus.
     - **Proxy-Einstellungen konfigurieren:** Legen Sie die IP-Adresse oder den Hostnamen des Proxy-Servers und die Portnummer fest. Wenn der Server, den Sie angegeben haben, Authentifizierung erfordert, klicken Sie auf die Option "Proxy-Server erfordert Authentifizierung" und geben Sie die Anmeldeinformationen ein.

       Klicken Sie auf "OK", um zur Konfiguration der Aktualisierung zurückzukehren.
   - **Staging-Server**: Wenn Sie diese Option auswählen, klicken Sie auf "Server hinzufügen", um einen Staging-Server zur Liste hinzuzufügen. Geben Sie seinen Hostnamen und die Portnummer ein, und klicken Sie auf "OK".

     Wenn Sie mehrere Staging-Server angeben, versucht die Anwendung, den ersten der aufgelisteten Server zu verwenden. Wenn die Verbindung erfolgreich ist, werden die verbleibenden aufgelisteten Server nicht für das Staging verwendet.
5. (Optional) Klicken Sie auf "Verbindung testen", um die Serververbindung zu überprüfen und warten Sie, bis der Test abgeschlossen ist.

6. (Optional) Klicken Sie auf die Option "Automatisch nach Aktualisierungen suchen" und legen Sie den Tag und die Zeit fest. Sie können einen täglichen oder wöchentlichen Ablaufplan angeben.

Klicken Sie auf "Speichern", um die Konfiguration der Aktualisierung anzuwenden.

Proxy-Einstellungen konfigurieren

CA ARCserve Central Applications lässt Sie einen Proxy-Server zur Kommunikation mit CA Support festlegen, um nach verfügbaren Aktualisierungen zu überprüfen und sie herunterzuladen. Um diese Möglichkeit zu aktivieren, geben Sie den Proxy-Server an, mit dem Sie anstelle des CA ARCserve Central Applications-Servers kommunizieren wollen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Konfiguration".

   Die Konfigurationsoptionen werden angezeigt.

2. Klicken Sie auf "Konfiguration aktualisieren".

   Die Optionen für die Aktualisierung der Konfiguration werden angezeigt.

3. Klicken Sie auf Proxy-Einstellungen.

   Das Dialogfeld "Proxy-Einstellungen" wird geöffnet.

4. Aktivieren Sie eine der folgenden Optionen:

   - **Proxy-Einstellungen des Browsers verwenden:** Lässt die Anwendung die gleichen Proxy-Einstellungen erkennen und verwenden, die auf den Browser angewendet werden, um für den Erhalt von Aktualisierungsinformationen mit dem CA Technologies-Server zu kommunizieren.

     Hinweis: Dieses Verhalten bezieht sich nur auf Internet Explorer- und Chrome-Browser.

   - **Proxy-Einstellungen konfigurieren:** Lässt Sie einen alternativen Server festlegen, den die Anwendung verwenden wird, um mit CA Support zu kommunizieren und nach Aktualisierungen zu prüfen. Der alternative Server (Proxy) hilft dabei, mehr Sicherheit, erhöhte Leistung und Verwaltungskontrolle zu bieten.

Füllen Sie die folgenden Felder aus:

- **Proxy-Server:** Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers an.
- **Port:** Geben Sie die Portnummer an, die der Proxy-Server verwenden wird, um mit der CA Support-Website zu kommunizieren.
- **(Optional) Proxy-Server erfordert Authentifizierung:** Falls die Anmeldeinformationen für den Proxy-Server nicht die gleichen sind wie die Anmeldeinformationen für den CA ARCserve Central Applications-Server, aktivieren Sie das Kontrollkästchen neben "Proxy-Server erfordert Authentifizierung" und legen Sie den Benutzernamen und das Kennwort fest, die erforderlich sind, um sich beim Proxy-Server anzumelden.

  Hinweis: Verwenden Sie das folgende Format, um den Benutzernamen anzugeben: <Domänenname>\<Benutzername>.

Klicken Sie auf "OK".

Die Proxy-Einstellungen sind konfiguriert.

Konfigurieren von Voreinstellungen für Social Networking

CA ARCserve Central Applications lässt Sie die Social Networking-Tools verwalten, die Ihnen dabei helfen, die Anwendung zu verwalten. Sie können Nachrichten-Feeds generieren, Verknüpfungen zu beliebten Social Networking-Websites angeben und Videoquellen-Websites auswählen.

So konfigurieren Sie Voreinstellungen für Social Networking

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Konfiguration".

   Der Bildschirm "Konfiguration" wird angezeigt.

2. Klicken Sie im Konfigurationsbereich auf "Konfiguration der Voreinstellungen".

   Die Optionen der Voreinstellungen werden angezeigt.

3. Legen Sie die benötigten Optionen fest.

   - **Nachrichten-Feed:** Ermöglicht es, dass die Anwendung RSS-Feeds über mit CA ARCserve Central Applications und CA ARCserve D2D in Zusammenhang stehenden Nachrichten und Produktinformationen (aus dem Expertenforum) anzeigt. Die Feeds werden auf der Startseite angezeigt.
   - **Social Networking:** Ermöglicht es, dass die Anwendung auf der Startseite Zugriffssymbole auf Twitter und Facebook für mit CA ARCserve Central Applications und CA ARCserve D2D im Zusammenhang stehende Social Networking-Websites anzeigt.
   - **Videos:** Ermöglicht es Ihnen, den Videotyp auszuwählen, um Ihre Produkte von CA ARCserve Central Applications und CA ARCserve D2D anzuzeigen. ("YouTube-Videos verwenden" ist das Standardvideo.)

   Klicken Sie auf "Speichern".

   Die Social Networking-Optionen werden angewendet.

4. Klicken Sie in der Navigationsleiste auf "Start".

   Die Startseite wird geöffnet.

5. Aktualisieren Sie Ihren Browser.

   Die Social Networking-Optionen werden angewendet.

Ändern des Administratorkontos

CA ARCserve Central Applications lässt Sie den Benutzernamen, das Kennwort, oder beides für das Administratorkonto ändern, nachdem Sie die Anwendung installiert haben. Dieses Administratorkonto wird im Anmeldefenster nur für den standardmäßigen Anzeigebenutzernamen verwendet.

Hinweis: Der angegebene Benutzername muss ein Windows-Administratorkonto oder ein Konto sein, das Windows-Administratorrechte hat.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Konfiguration".

   Die Konfigurationsoptionen werden angezeigt.

2. Klicken Sie auf "Administratorkonto".

3. Die Administratorkontoeinstellungen werden angezeigt.
4. Aktualisieren Sie folgende Felder je nach Bedarf:
   - Benutzername
   - Kennwort

   Klicken Sie auf "Speichern".

Das Administratorkonto wurde geändert.

Konfigurieren der Einstellungen für die Bereitstellung von D2D

Mit CA ARCserve Central Protection Manager können Sie die Einstellungen für die Bereitstellung von D2D für den Speicherort, an dem Sie CA ARCserve D2D bereitstellen möchten, konfigurieren.

Hinweis: Um CA ARCserve D2D auf Computern mit Windows XP bereitzustellen, deaktivieren Sie auf dem Remote-Computer mit Windows XP die Option "Einfache Dateifreigabe verwenden".

So konfigurieren Sie die Einstellungen für die Bereitstellung von D2D

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Konfiguration".

   Der Bildschirm "Konfiguration" wird angezeigt.
2. Klicken Sie im Konfigurationsbereich auf "Konfiguration der D2D-Bereitstellung".

   Die Option "Konfiguration der D2D-Bereitstellung" wird angezeigt.

3. Füllen Sie im Bildschirm "Konfiguration" folgende Felder aus:
   - **Port**: Diese Portnummer wird verwendet, um eine Verbindung zur webbasierten Benutzeroberfläche herzustellen. Standardmäßig wird die Portnummer 8014 angegeben.
   - **Installationspfad:** Dies ist der Installationspfad auf dem Remote-Server für CA ARCserve D2D. Der Standardspeicherort ist %Programme%.
   - **Setup erlauben, den Treiber zu installieren** (standardmäßig ausgewählt): Legen Sie fest, ob Setup den Treiber automatisch installieren soll.
   - **Neu starten** (standardmäßig "Ja"): Legen Sie fest, ob der erforderliche Neustart nach Abschluss der Bereitstellung automatisch durchgeführt oder später manuell gestartet werden soll.
   - **HTTPS verwenden** (standardmäßig "Nein"): HTTPS (sicher) bietet eine höhere Sicherheitsebene als HTTP-Kommunikation. HTTPS ist das empfohlene Kommunikationsprotokoll, wenn Sie in Ihrem Netzwerk vertrauliche Informationen übertragen.
4. Klicken Sie auf "Speichern".

Die Bereitstellung der D2D-Konfiguration wird angewendet.

Konfigurieren der Datenbank

Nachdem Sie CA ARCserve Central Protection Manager installiert haben, können Sie Folgendes durchführen:

- Aktualisieren Sie die Einstellungen für die CA ARCserve Central Protection Manager-Datenbank. Zum Beispiel können Sie unter anderem den Namen der Instanz oder die Port-Werte aktualisieren.
- Ändern Sie die CA ARCserve Central Protection Manager-Datenbankanwendung zu Microsoft SQL Server.
- Ändern Sie die CA ARCserve Central Protection Manager-Datenbankanwendung zu Microsoft SQL Server Express Edition.

So konfigurieren Sie die CA ARCserve Central Protection Manager-Datenbank:

1. Klicken Sie in der Navigationsleiste auf "Konfiguration".
2. Klicken Sie im Konfigurationsbereich auf "Datenbankkonfiguration".
3. Füllen Sie im Bildschirm "Konfiguration" folgende Felder aus:
   - **SQL Server-Rechnername:** Geben Sie den Namen des Servers an, der die SQL Server-Instanz hostet.
   - **SQL Server-Instanz:** Geben Sie den Namen der SQL Server-Instanz an.
   - **SQL Server-Port:** Geben Sie die Portnummer für diese Instanz an oder aktivieren Sie die Option "Automatisch erkennen".
   - **Authentifizierungsmodus auswählen:** Der Windows-Authentifizierungsmodus ist die Standardauswahl.

     Hinweis: Die Auswahl von SQL Server und Windows-Authentifizierungsmodus aktiviert die Felder "Benutzername" und "Kennwort".
   - (Optional) **Test:** Klicken Sie auf "Test", um zu überprüfen, ob die Anwendung mit der Microsoft SQL Serverinstanz kommunizieren kann.
   - **Geben Sie die Werte für das Datenbankverbindungs-Pool an:** Die Werte für "Max. Verbindungen" und "Min. Verbindungen" müssen zwischen 1 und 99 liegen.
4. Klicken Sie auf "Speichern".

   Hinweis: Klicken Sie auf "Zurücksetzen", um alle festgelegten Werte zu löschen und die ursprünglichen Daten zu laden.
5. (Optional) Wenn die Anwendung Daten für CA ARCserve Central Reporting zur Verfügung stellt, öffnen Sie Windows Server Manager und starten Sie den folgenden Dienst neu:

   `CA ARCserve Central Applications Service`

   Die Datenbankserver-Konfiguration wird angewendet.

CA ARCserve Central Protection Manager-Datenbank erneut erstellen

Aus verschiedenen Gründen möchten Sie die CA ARCserve Central Protection Manager-Datenbank möglicherweise erneut erstellen. Zum Beispiel verbraucht Ihre aktuelle Datenbank mehr als 10 GB an Daten. Im Folgenden wird erläutert, wie die CA ARCserve Central Protection Manager-Datenbank erneut erstellt wird. Der Vorgang bezieht sich auf Datenbanken von Microsoft SQL Server und Microsoft SQL Server Express Edition.

Wichtig! Wenn Sie die CA ARCserve Central Protection Manager-Datenbank löschen, gehen alle aktuellen Daten verloren.

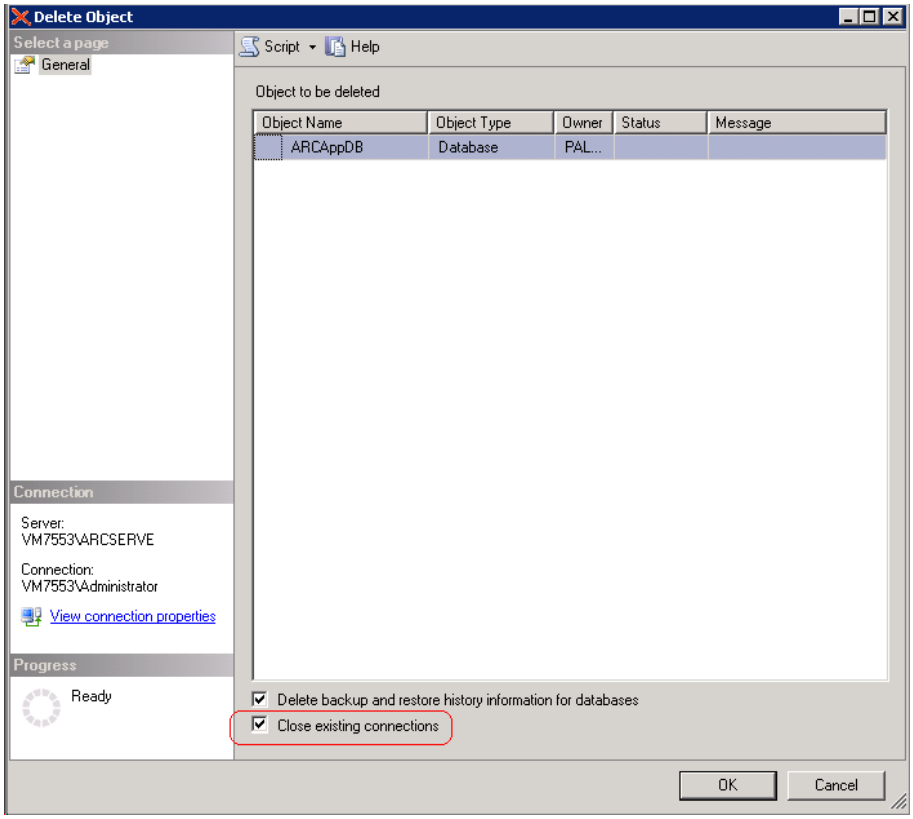
So erstellen Sie die CA ARCserve Central Protection Manager-Datenbank erneut

1. Öffnen Sie Microsoft SQL Server Management Studio Express, und melden Sie sich bei der Instanz "ARCserve_APP" an.

   Hinweis: Wenn Microsoft SQL Server Management Studio Express nicht auf dem CA ARCserve Central Protection Manager-Server installiert ist, können Sie das Hilfsprogramm vom Microsoft Download Center herunterladen.

2. Klicken Sie mit der rechten Maustaste auf "ARCAppDB", und klicken Sie im Kontextmenü auf die Option "Löschen".

   Das Dialogfeld "Objekt löschen" wird angezeigt.



3. Klicken Sie im Dialogfeld "Objekt löschen" auf die Option "Bestehende Verbindungen schließen", und klicken Sie auf "OK".

   Das Dialogfeld "Objekt löschen" wird geschlossen, und die CA ARCserve Central Protection Manager-Datenbank wird gelöscht.

4. Öffnen Sie CA ARCserve Central Protection Manager, und klicken Sie in der Navigationsleiste auf "Konfiguration".

   Die Konfigurationsoptionen werden angezeigt.

5. Klicken Sie auf "Datenbankkonfiguration".

   Die Datenbankoptionen werden angezeigt.

6. Stellen Sie sicher, dass die in den folgenden Feldern angegebenen Werte korrekt sind:
   - **SQL Server-Rechnername:** Geben Sie den Namen des Servers an, der die SQL Server-Instanz hostet.
   - **SQL Server-Instanz:** Geben Sie den Namen der SQL Server-Instanz an.
7. (Optional) Füllen Sie die folgenden Felder aus:
   - **SQL Server-Port:** Geben Sie die Portnummer für diese Instanz an oder aktivieren Sie die Option "Automatisch erkennen".
   - **Authentifizierungsmodus auswählen:** Der Windows-Authentifizierungsmodus ist die Standardauswahl.

     Hinweis: Die Auswahl von SQL Server und Windows-Authentifizierungsmodus aktiviert die Felder "Benutzername" und "Kennwort".
   - **Geben Sie die Werte für das Datenbankverbindungs-Pool an:** Die Werte für "Max. Verbindungen" und "Min. Verbindungen" müssen zwischen 1 und 99 liegen.
8. Klicken Sie auf "Testen", um eine Verbindung zur Datenbank herzustellen.
9. Klicken Sie auf "Speichern".

CA ARCserve Central Protection Manager erstellt die Datenbank erneut. Der Name der Datenbankinstanz ist "ARCAppDB".

Kapitel 4: Verwenden von CA ARCserve Central Protection Manager

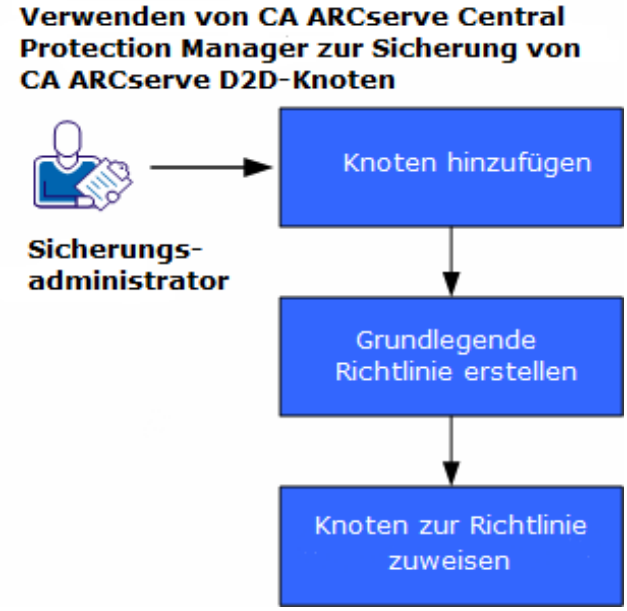
Dieses Kapitel enthält folgende Themen:

Verwenden von CA ARCserve Central Protection Manager zur Sicherung von CA ARCserve D2D-Knoten (siehe Seite 50)
So verwalten Sie Knoten in CA ARCserve Central Protection Manager (siehe Seite 57)
Verwalten von CA ARCserve D2D-Richtlinien (siehe Seite 88)
Sicherung jetzt ausführen (siehe Seite 141)
Anzeigen von Jobstatusinformationen (siehe Seite 143)
Wiederherstellen von Knoten in CA ARCserve Central Protection Manager (siehe Seite 144)
Anzeigen von CA ARCserve Central Protection Manager-Protokollen (siehe Seite 164)
Links zur Navigationsleiste hinzufügen (siehe Seite 166)
Best Practices (siehe Seite 167)
Ändern des Server-Kommunikationsprotokolls (siehe Seite 168)

Verwenden von CA ARCserve Central Protection Manager zur Sicherung von CA ARCserve D2D-Knoten

Mithilfe von CA ARCserve Central Protection Manager können Sie Richtlinien erstellen, die bestimmen, wie und wann Daten, die sich auf CA ARCserve D2D-Knoten befinden, gesichert und gespeichert werden. Die in den folgenden Themen enthaltenen Informationen beschreiben, wie Sie CA ARCserve D2D-Sicherungsjobs mithilfe einer grundlegenden Richtlinie übergeben können. Grundlegende Richtlinien können die meisten CA ARCserve D2D-Knoten schützen, die in Produktionsumgebungen funktionieren.

Das folgende Diagramm veranschaulicht den Prozess des Verwendens von CA ARCserve Central Protection Manager, um eine grundlegende Sicherungsrichtlinie zu erstellen und CA ARCserve D2D-Knoten zu sichern:


Verwenden von CA ARCserve Central Protection Manager zur Sicherung von CA ARCserve D2D-Knoten
Sicherungs-administrator
Knoten hinzufügen
Grundlegende Richtlinie erstellen
Knoten zur Richtlinie zuweisen

Folgen Sie diesen Schritten, um CA ARCserve Central Protection Manager dazu zu verwenden, eine grundlegende Richtlinie zu erstellen und CA ARCserve D2D-Knoten zu sichern:

1. Knoten hinzufügen (siehe Seite 51)
2. Grundlegende Richtlinie erstellen (siehe Seite 51)
3. Knoten zu Richtlinien zuweisen (siehe Seite 56)

Hinzufügen von Knoten

Um CA ARCserve D2D-Knoten mithilfe einer Richtlinie zu sichern, bestimmen Sie zuerst die Knoten, die Sie sichern wollen.

Hinweis: Sie können Discovery verwenden, um diese Aufgabe zu automatisieren. Allerdings erkennt Discovery nur die Knoten, die im Active Directory auf Active Directory-Servern angezeigt werden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA ARCserve Central Protection Manager an, und klicken Sie in der Navigationsleiste auf "Knoten".
2. Klicken Sie in der Symbolleiste "Knoten" auf "Hinzufügen", und dann im Pop-up-Menü auf "Knoten nach IP/Namen hinzufügen".
3. Vervollständigen Sie alle Felder des Dialogfelds "Knoten nach IP/Namen hinzufügen" und klicken Sie auf "OK".
4. (Optional) Wenn der neu hinzugefügte Knoten nicht in der Knotenliste angezeigt wird, klicken Sie in der Symbolleiste "Knoten" auf "Aktualisieren".

   Hinweis: Um weitere Knoten hinzuzufügen, wiederholen Sie die Schritte 2, 3 und 4.

Nachdem der Knoten hinzugefügt worden ist, wird er in den Standardgruppen angezeigt.

Grundlegende Richtlinie erstellen

Richtlinien bestimmen, wie und wann Daten, die sich auf CA ARCserve D2D-Knoten befinden, gesichert und gespeichert werden. CA ARCserve Central Protection Manager enthält keine Standardrichtlinien. Das Erstellen einer Richtlinie ist eine erforderliche Aufgabe für das Sichern von Daten, die sich auf Knoten befinden.

Um eine grundlegende Richtlinie zu erstellen, geben Sie die Schutzeinstellungen an und erstellen Sie einen Ablaufplan. Schutzeinstellungen legen die Daten fest, die Sie sichern wollen, und wo und wie die Daten gespeichert werden sollen. Der Ablaufplan legt fest, wann und wie oft die Knoten gesichert werden.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite von CA ARCserve Central Protection Manager in der Navigationsleiste auf "Richtlinien", um das Fenster "Richtlinien" zu öffnen.
2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.
3. Geben Sie im Feld "Richtlinienname" auf dem Dialogfeld "Neue Richtlinie" einen Namen für die Richtlinie an.

4. Klicken Sie auf die Registerkarte "Sicherungseinstellungen" und klicken Sie dann auf "Schutzeinstellungen", um die Optionen der Schutzeinstellungen anzuzeigen.

5. Geben Sie das Sicherungsziel an.

   Sie können einen lokalen Pfad (Volume oder Ordner) oder einen freigegebenen Remote-Ordner (oder zugeordnetes Laufwerk) als Sicherungsziel angeben.

   - Wenn Sie die Sicherung in Ihrem lokalen Pfad (Volume oder Ordner) speichern, darf das ausgewählte Sicherungsziel nicht mit der Sicherungsquelle identisch sein. Wenn Sie die Quelle unabsichtlich in das ausgewählte Ziel aufnehmen, ignoriert der Sicherungsjob diesen Teil der Quelle und nimmt ihn nicht in die Sicherung auf.

     Wichtig! Stellen Sie sicher, dass Ihr angegebenes Zielvolume keine Systeminformationen enthält. CA ARCserve D2D sichert keine Zielvolumes, die Systeminformationen enthalten. Wenn Sie versuchen, den Computer mithilfe von Bare-Metal-Recovery (BMR) wiederherzustellen, schlägt die Wiederherstellung möglicherweise fehl.

     Hinweis: Dynamische Datenträger können nicht auf Datenträgerebene wiederhergestellt werden. Wenn Ihre Daten auf einem Volume eines dynamischen Datenträgers gesichert sind, können Sie diesen dynamischen Datenträger während der Bare-Metal-Recovery nicht wiederherstellen.

   - Wenn Sie Daten auf einem freigegebenen Remote-Speicherort sichern, geben Sie einen Speicherort und die Anmeldeinformationen an, die erforderlich sind, um auf den Remote-Rechner zuzugreifen.

6. Geben Sie die Sicherungsquelle an.

   Sie können den gesamten Knoten oder einzelne Volumes auf Ihrem Knoten für die Sicherung angeben.

   Beachten Sie Folgendes:

   - Wenn die Option zur Sicherung des gesamten Rechners ausgewählt wird, erkennt CA ARCserve D2D automatisch alle Datenträger/Volumes, die an den derzeitigen Rechner angeschlossen sind und nimmt sie in die Sicherung auf.
   - Wenn System-/Startvolume nicht für die Sicherung ausgewählt ist, wird eine Warnmeldung angezeigt. Die Meldung zeigt an, dass die Sicherung nicht für BMR verwendet werden kann.

7. Geben Sie die Wiederherstellungspunkte an.

   Legt die Menge der aufbewahrten Sicherungs-Images fest. Der Standard ist 31 und die Höchstzahl ist 1344. Wenn diese Menge geändert wird, beachten Sie den verfügbaren freien Speicherplatz auf dem Ziel.

   Wenn die festgelegte Anzahl an Wiederherstellungspunkten überschritten wird, fügt CA ARCserve D2D die älteste inkrementelle untergeordnete Sicherung zur übergeordneten Sicherung hinzu und stellt das Baseline-Image wieder her. Das neue Baseline-Image besteht aus den Blöcken, für die die Beschreibung "übergeordnetes Objekt plus ältestes untergeordnetes Objekt" gilt. Der Zyklus des Einfügens der ältesten untergeordneten Sicherung in die übergeordnete Sicherung wiederholt sich für jede nachfolgende Sicherung. Dieser Prozess lässt Sie zahllose Zuwachssicherungen ausführen, während Sie die gleiche Aufbewahrungsanzahl beibehalten.

8. Geben Sie den Komprimierungstyp an, den Sie für Sicherungen verwenden möchten.

   Durch eine Komprimierung wird der verwendete Speicherplatz verringert. Dies hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit der Sicherung.

   Es stehen folgende Komprimierungsoptionen zur Verfügung:

   Keine Komprimierung

   Es wird keine Komprimierung durchgeführt. Diese Option bedeutet niedrigste CPU-Auslastung (höchste Geschwindigkeit), aber auch höchste Speicherplatzverwendung für Ihr Sicherungs-Image.

   Standard-Komprimierung

   Es wird eine Komprimierung bis zu einem gewissen Grad ausgeführt. Diese Option bietet ein Gleichgewicht zwischen CPU-Auslastung und verwendetem Speicherplatz. Standardmäßige Komprimierung ist die Standardeinstellung.

   Maximale Komprimierung

   Es wird eine maximale Komprimierung durchgeführt. Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigste Speicherplatzverwendung für Ihr Sicherungs-Image.

   Beachten Sie Folgendes:

   - Wenn Ihr Sicherungs-Image nicht komprimierbare Daten wie z. B. JPG- oder ZIP-Dateien enthält, muss für die Verarbeitung dieser Daten zusätzlicher Speicherplatz zugewiesen werden.
   - Wenn auf Ihrem Ziel nicht genügend freier Speicherplatz zur Verfügung steht, sollten Sie in Betracht ziehen, die Einstellung "Komprimierung" der Sicherung zu erhöhen.

9. Geben Sie die Verschlüsselungseinstellungen an, die Sie zur zusätzlichen Sicherheit verwenden wollen.

   a. Wählen Sie den Typ des Verschlüsselungsalgorithmus aus, den Sie für Sicherungen verwenden möchten.

      Bei der Datenverschlüsselung werden Daten in ein Format umgewandelt, das ohne den entsprechenden Entschlüsselungsmechanismus nicht verständlich ist. CA ARCserve D2D-Datenschutz verwendet sichere AES-Verschlüsselungsalgorithmen (AES steht im Englischen für Advanced Encryption Standard), um größtmögliche Sicherheit und Datenschutz für Ihre angegebenen Daten zu erreichen.

      Die verfügbaren Formatoptionen sind "Keine Verschlüsselung", "AES-128", "AES-192" und "AES-256". (Um die Verschlüsselung zu deaktivieren, wählen Sie "Keine Verschlüsselung" aus).

      - Eine vollständige Sicherung und alle verknüpften Zuwachs- und Überprüfungssicherungen müssen den gleichen Verschlüsselungsalgorithmus verwenden.
      - Wenn Sie den Verschlüsselungsalgorithmus für eine Zuwachs- oder Überprüfungssicherung ändern, sollten Sie eine vollständige Sicherung ausführen. Dies bedeutet, dass nach einer Änderung des Verschlüsselungsalgorithmus die erste Sicherung trotz des ursprünglichen Sicherungstyps vollständig ist.

        Wenn Sie zum Beispiel das Algorithmusformat ändern und eine angepasste Zuwachs- oder Überprüfungssicherung manuell übergeben, wird automatisch auf eine vollständige Sicherung gewechselt.

   b. Wenn ein Verschlüsselungsalgorithmus ausgewählt wird, müssen Sie ein Verschlüsselungskennwort angeben (und es bestätigen).

      - Das Verschlüsselungskennwort kann höchstens aus 23 Zeichen bestehen.
      - Eine vollständige Sicherung und alle verknüpften Zuwachs- und Überprüfungssicherungen müssen das gleiche Kennwort zur Datenverschlüsselung verwenden.
      - Wenn Sie das Verschlüsselungskennwort für eine Zuwachs- oder Überprüfungssicherung ändern, sollten Sie eine vollständige Sicherung ausführen. Dies bedeutet, dass nach einer Änderung des Verschlüsselungskennworts die erste Sicherung trotz des ursprünglichen Sicherungstyps vollständig ist.

        Wenn Sie zum Beispiel das Verschlüsselungskennwort ändern und eine angepasste Zuwachs- oder Überprüfungssicherung manuell übergeben, wird automatisch auf eine vollständige Sicherung gewechselt.

   Wenn Verschlüsselung aktiviert ist, wird das Aktivitätsprotokoll aktualisiert, um die verwendete Verschlüsselung für jede Sicherung zu beschreiben.

10. Machen Sie Angaben zu "Sicherung drosseln".

    Sie können die Höchstgeschwindigkeit festlegen (MB/Min), mit der Sicherungen geschrieben werden. Sie können die Sicherungsgeschwindigkeit drosseln, um die CPU- oder Netzwerkauslastung zu reduzieren. Allerdings beeinflusst das Einschränken der Sicherungsgeschwindigkeit das Sicherungszeitfenster negativ.

11. Klicken Sie auf die Registerkarte "Ablaufplan", um die Optionen für den Ablaufplan anzuzeigen.

12. Festlegen des Sicherungsablaufplans:

    Startzeitpunkt festlegen

    Legt den Startzeitpunkt (Datum und Uhrzeit) Ihrer geplanten Sicherungen fest.

    Zuwachssicherung

    Legt den Ablaufplan für Zuwachssicherungen fest.

    Es stehen die Optionen "Wiederholen" und "Nie" zur Verfügung. Wenn Sie "Wiederholen" auswählen, müssen Sie auch die Zeitspanne (Minuten, Stunden oder Tage) zwischen den Sicherungsversuchen festlegen. Das Mindestintervall für Zuwachssicherungen ist 15 Minuten.

    Standardmäßig sind tägliche Zuwachssicherungen geplant.

    Vollständige Sicherung

    Legt den Ablaufplan für vollständige Sicherungen fest.

    CA ARCserve D2D führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke des Quellrechners durch. Es stehen die Optionen "Wiederholen" und "Nie" zur Verfügung. Wenn Sie "Wiederholen" auswählen, müssen Sie auch die Zeitspanne (Minuten, Stunden oder Tage) zwischen den Sicherungsversuchen festlegen. Das Mindestintervall für vollständige Sicherungen ist 15 Minuten.

    Standardmäßig ist der Ablaufplan für vollständige Sicherungen "Nie" (keine Wiederholung geplant).

    Überprüfungssicherung

    Legt den Ablaufplan für Überprüfungssicherungen fest.

    Es stehen die Optionen "Wiederholen" und "Nie" zur Verfügung. Wenn Sie "Wiederholen" auswählen, müssen Sie auch die Zeitspanne (Minuten, Stunden oder Tage) zwischen den Sicherungsversuchen festlegen. Das Mindestintervall für Überprüfungssicherungen ist 15 Minuten.

    Standardmäßig ist der Ablaufplan für Überprüfungssicherungen "Nie" (keine Wiederholung geplant).

13. Klicken Sie auf "Speichern".

Die grundlegende Sicherungsrichtlinie wurde erstellt. Die Richtlinie wird in der Liste der Richtlinien unter dem Namen angezeigt, den Sie in Schritt 3 des Fensters "Richtlinien" angegeben haben.

Hinweis: Wenn für denselben Zeitpunkt mehrere Sicherungstypen geplant sind, gelten die folgenden Prioritäten:

- Priorität 1 - Vollständige Sicherung
- Priorität 2 - Überprüfungssicherung
- Priorität 3 - Zuwachssicherung

Beispiel: Wenn alle drei Sicherungstypen zur gleichzeitigen Ausführung geplant sind, führt CA ARCserve D2D die vollständige Sicherung aus. CA ARCserve D2D führt Überprüfungssicherungen aus, wenn Überprüfungssicherungen und Zuwachssicherungen zur gleichzeitigen Ausführung geplant sind, jedoch keine vollständigen Sicherungen geplant sind. Eine geplante Zuwachssicherung wird nur dann durchgeführt, wenn keine Konflikte mit anderen Sicherungstypen bestehen.

Knoten zu Richtlinien zuweisen

Nachdem Sie die grundlegende Richtlinie erstellt haben, weisen Sie die CA ARCserve D2D-Knoten zu, die Sie unter Verwendung der Richtlinie sichern wollen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite von CA ARCserve Central Protection Manager in der Navigationsleiste auf "Richtlinien", um das Fenster "Richtlinien" zu öffnen.
2. Klicken Sie auf dem Fenster "Richtlinie" in der Liste der Richtlinien auf die Richtlinie, die Sie erstellt haben.
3. Klicken Sie auf die Registerkarte "Richtlinienzuweisung", um die Richtlinienzuweisung anzuzeigen (Liste).
4. Klicken Sie auf "Zuweisen und Zuweisung aufheben", um "Zuweisung der Richtlinie durchführen/aufheben" zu öffnen.
5. Um Knoten hinzuzufügen, aktivieren Sie die Kontrollkästchen des oder der Knoten, die Sie hinzufügen möchten, und klicken Sie auf den Rechtspfeil.

   Das Dialogfeld "Lizenzvereinbarung" wird geöffnet.

6. Lesen und akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf "Abgeschlossen".

   Die Knoten werden der Richtlinie zugewiesen, die Sie erstellt haben, und unmittelbar bereitgestellt. Sicherungen starten auf der Basis des Ablaufplans, den Sie auf der Registerkarte "Ablaufplan" festgelegt haben.

7. Wenn Sie mit der Zuweisung von Knoten zu Richtlinien fertig sind, klicken Sie auf "OK", um die Richtlinienzuweisungen zu speichern und schließen Sie das Dialogfeld "Zuweisen und Zuweisung aufheben" .

Nachdem die Knoten zugewiesen wurden, stellt
CA ARCserve Central Protection Manager die Richtlinie unmittelbar auf den Knoten bereit. Die Sicherungsvorgänge starten auf der Basis der Schutzeinstellungen, die Sie ausgewählt haben, und folgen dem Ablaufplan, den Sie in Ihrer Richtlinie festgelegt haben.

So verwalten Sie Knoten in CA ARCserve Central Protection Manager

CA ARCserve Central Protection Manager stellt verschiedene Tools und Optionen bereit, mit denen Sie Knoten und Knotengruppen verwalten können. Dieser Abschnitt enthält Informationen darüber, wie Sie Synchronisationsdaten für Knoten und Knotengruppen hinzufügen, löschen und ändern können. Sie können auch eine Discovery ausführen und CA ARCserve D2D auf Knoten bereitstellen.

Dieser Abschnitt enthält folgende Themen:

Aufbau des Fensters "Knotenverwaltung" (siehe Seite 58)
Funktionen für Knoten (siehe Seite 60)
Funktionen für Knotengruppen (siehe Seite 77)
Mithilfe von Discovery nach Knoten suchen (siehe Seite 82)
CA ARCserve D2D-Bereitstellungsaufgaben (siehe Seite 83)
Filtern von Knotengruppen (siehe Seite 87)

Aufbau des Fensters "Knotenverwaltung"

"Knotenverwaltung" ist eine Eingabekomponente von CA ARCserve Central Applications. Sie können von der Navigationsleiste aus im linken Bereich der CA ARCserve Central Protection Manager-Anwendung darauf zugreifen.

Der Bildschirm "Knotenverwaltung" enthält vier Kategorien, in denen Sie arbeiten können:

- **Knoten:** Lässt Sie bestimmte Knoten verwalten. Weitere Informationen über das Verwalten von Knoten finden Sie unter Funktionen für Knoten (siehe Seite 60).
- **Knotengruppe:** Lässt Sie bestimmte Knotengruppen verwalten. Weitere Informationen finden Sie unter Funktionen für Knotengruppen (siehe Seite 77).
- **Aktionen:** Sie können Daten sichern (siehe Seite 141), Daten wiederherstellen (siehe Seite 144) und Daten bereitstellen (siehe Seite 84).
- **Filter:** Lässt Sie Filter verwenden, um Knoten in einer Gruppe anzuzeigen, auf der eine bestimmte Anwendung installiert ist. Weitere Informationen finden Sie unter Filtern von Knotengruppen (siehe Seite 87).

Der Status jedes der Knoten in der Spalte der Produkte bestimmt CA ARCserve Backup- und CA ARCserve D2D-Symbole. Die folgende Tabelle beschreibt die Status für jedes Produkt in der Produktspalte:

Symbol	Beschreibung
	Dieser Status mit dem Buchstaben "M" zeigt an, dass der Knoten ein von CA ARCserve Central Applications verwalteter CA ARCserve Backup-Primär- oder -Standalone-Server ist.
	Dieser Status mit dem Buchstaben "M" und einem Ausrufezeichen rechts unten zeigt an, dass der Knoten ein von CA ARCserve Central Applications verwalteter CA ARCserve Backup-Primär- oder -Standalone-Server ohne erfolgreiche Synchronisation in den letzten "xx" Stunden ist. ('xx' beträgt standardmäßig 48 Stunden) oder die Synchronisation wurde noch nicht ausgeführt.
	Dieser Status ohne den Buchstaben "M" zeigt an, dass der Knoten ein nicht von CA ARCserve Central Applications verwalteter CA ARCserve Backup-Primär-, -Standalone- oder -Mitgliedsserver ist.
	Dieser Status zeigt an, dass dieser Knoten eine ältere CA ARCserve Backup-Version enthält
	Dieser Status zeigt an, dass der Knoten nicht von CA ARCserve Central Applications verwaltet wird und sich nicht mit CA ARCserve D2D verbinden kann.
	Dieser Status zeigt an, dass dieser Knoten eine ältere CA ARCserve D2D-Version enthält.
	Dieser Status mit dem Buchstaben "M" zeigt an, dass der Knoten von CA ARCserve Central Applications verwaltet wird und mit CA ARCserve D2D verbunden ist.
	Dieser Status mit dem Buchstaben "M" zeigt an, dass der Knoten von CA ARCserve Central Applications verwaltet wird und nicht mit CA ARCserve D2D verbunden werden kann.
	Dieser Status mit dem Buchstaben "M" zeigt an, dass der Knoten von CA ARCserve Central Applications verwaltet wird und unter Warnungen mit CA ARCserve D2D verbunden ist.
	Dieser Status mit dem Buchstaben "M" und einem Ausrufezeichen unten rechts zeigt an, dass der Knoten ein von CA ARCserve Central Applications verwalteter CA ARCserve D2D-Server ohne erfolgreiche Synchronisation in den letzten "xx" Stunden ist. ('xx' beträgt standardmäßig 48 Stunden) oder die Synchronisation wurde noch nicht ausgeführt.

Funktionen für Knoten

CA ARCserve Central Protection Manager lässt Sie Knoten hinzufügen, ändern und löschen, Daten synchronisieren, Knoteneinstellungen festlegen, Knoten erkennen, Knoteninformationen in eine CSV-Datei exportieren und den Status jedes Knotens bestimmen.

Hinweis: Wenn Sie Knoten mit übereinstimmenden CA ARCserve Backup- und CA ARCserve D2D-Servern zu CA ARCserve Central Protection Manager hinzufügen und an jedem Knoten eine Synchronisation ausführen, werden die Daten für den jeweiligen Knoten generiert und können in CA ARCserve Central Reporting angezeigt werden. Weitere Details über Synchronisation finden Sie in den Synchronisationsdaten und -optionen (siehe Seite 72).

Knoten mithilfe von Discovery hinzufügen

CA ARCserve Central Protection Manager lässt Sie mehrere Knoten aus Discovery-Ergebnissen hinzufügen.

So fügen Sie Knoten mithilfe von Discovery hinzu

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird geöffnet.

2. Klicken Sie auf der Knoten-Symbolleiste auf "Erkennen".

   Das Dialogfeld "Discovery nach Active Directory" öffnet sich.

3. Füllen Sie die folgenden Felder aus:

   - Benutzername (Domäne)
   - Kennwort (Domäne)
   - Computernamenfilter

   Klicken Sie auf "Hinzufügen" und anschließend auf "Discovery starten".

   Discovery (siehe Seite 61) wird ausgeführt.

4. Wenn das Erkennen von Knoten abgeschlossen ist, wird folgende Bestätigungsmeldung angezeigt:

   `Möchten Sie weitere Knoten aus dem Discovery-Ergebnis hinzufügen?`

   Klicken Sie auf "Ja", um zu "Knoten aus Discovery-Ergebnis hinzufügen" zu gelangen.

   Hinweis: Um die Meldung zu schließen, ohne Knoten hinzuzufügen, klicken Sie auf "Nein".

   Der Bildschirm "Knoten aus Discovery-Ergebnis hinzufügen" öffnet sich und zeigt eine Liste der erkannten Knoten an.

5. Wählen Sie aus der Liste "Erkannte Knoten" die Knoten aus, die Sie hinzufügen möchten, und klicken Sie auf den Pfeil, um sie zur Liste "Zu schützende Knoten" hinzuzufügen. Klicken Sie zum Abschluss auf "Weiter".

   Hinweis: Sie können die Liste nach Knotennamen oder Domäne filtern, um die Liste zu verkürzen.

6. (Optional) Wählen Sie einen oder mehrere Knoten aus und klicken Sie auf "Ausgewählte Knoten verbergen", um Knoten auszublenden, die Sie nicht sichern wollen.

7. (Optional) Aktivieren Sie die Option "Verborgene Knoten anzeigen", um verborgene Knoten wieder auf der Liste "Erkannte Knoten" anzuzeigen. Um die Knoten wieder auszublenden, deaktivieren Sie die Option.

8. Geben Sie im Fenster "Knoten-Anmeldeinformationen" einen Benutzernamen und ein Kennwort für den Knoten an, den Sie hinzufügen wollen. Sie können globale Anmeldeinformationen angeben oder Anmeldeinformationen auf die ausgewählten Knoten anwenden.

9. Klicken Sie auf Fertig stellen.

Die Knoten werden hinzugefügt.

Dialogfeld "Discovery-Überwachsungsserver"

Das Dialogfeld "Discovery-Überwachsungsserver" zeigt den Gesamtstatus der innerhalb Ihrer Umgebung erkannten Knoten an.

Das Dialogfeld "Discovery-Überwachsungsserver" enthält folgende Informationen:

Phase

Zeigt die drei Phasen an, Knoten zu erkennen: "Knoten wird erkannt", "Daten werden aktualisiert", und "Discovery abgeschlossen".

Status

Zeigt während des Discovery-Prozesses den Status "Aktiv" an und den Status "Abgeschlossen", wenn Discovery abgeschlossen ist.

Vergangene Zeit

Zeigt an, wie viel Zeit das Erkennen von Knoten in Anspruch genommen hat.

Anzahl der verarbeiteten Knoten

Zeigt die Anzahl der verarbeiteten Knoten an, die protokolliert und in der Datenbank aktualisiert wird.

Hinzufügen von Knoten nach IP-Adresse oder Knotennamen

Mit CA ARCserve Central Protection Manager können Sie CA ARCserve D2D- und CA ARCserve Backup-Knoten zu Knotengruppen hinzufügen, indem Sie die IP-Adresse oder den Hostnamen des Knotens angeben.

So fügen Sie Knoten nach IP-Adresse oder Knotennamen hinzu

1. Klicken Sie auf der Startseite in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt:

2. Klicken Sie in der Symbolleiste "Knoten" auf "Hinzufügen", und dann im Pop-up-Menü auf "Knoten nach IP/Namen hinzufügen".

   Das Dialogfeld "Knoten nach IP/Namen hinzufügen" wird geöffnet.

3. Füllen Sie folgende Felder im Dialogfeld "Knoten nach IP/Namen hinzufügen" aus:

   - **IP/Knotenname:** Lässt Sie die IP-Adresse oder den Namen des Knotens festlegen.
   - **Beschreibung:** Lässt Sie eine Beschreibung für den Knoten festlegen.
   - **Benutzername:** Lässt Sie den Benutzernamen festlegen, der für die Anmeldung am Knoten erforderlich ist.
   - **Kennwort:** Lässt Sie das Kennwort festlegen, das für die Anmeldung am Knoten erforderlich ist.

   Klicken Sie auf "OK".

4. (Optional) Wenn der neu hinzugefügte Knoten nicht in der Knotenliste angezeigt wird, klicken Sie in der Symbolleiste "Knoten" auf "Aktualisieren".

   Das Dialogfeld "Knoten nach IP/Namen hinzufügen" schließt sich und der Knoten ist hinzugefügt.

5. (Optional) Wenn CA ARCserve Backup auf dem Knoten installiert ist und die CA ARCserve Central Protection Manager-Anmeldeinformationen keine CA ARCserve Backup-Administratorrechte haben, wird folgende Meldung angezeigt:

   `ARCserve Backup-Administratorrechte sind erforderlich.`

   Legen Sie, um fortzufahren, die Anmeldeinformationen für das CA ARCserve Backup-Administratorkonto fest, und klicken Sie auf OK.

   Hinweis: CA ARCserve Central Protection Manager kann Datensynchronisation nur auf CA ARCserve Backup-Primärservern und eigenständigen Servern ausführen. Wenn der Primärserver ein Zweigstellenserver ist, kann CA ARCserve Central Protection Manager die CA ARCserve Backup-Daten nur mit dem globalen Dashboard-Server synchronisieren.

Der Knoten wird hinzugefügt.

Hinzufügen von Knoten vom Discovery-Ergebnis

Diese Option lässt Sie die Knoten auswählen, die automatisch erkannt werden auf der Basis der Einstellungen, die Sie im Feld "Discovery-Konfiguration" angegeben haben.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie in der Kategorie "Knoten" auf "Hinzufügen" und danach im Pop-up-Menü auf "Knoten aus Discovery-Ergebnis hinzufügen".

   Der Bildschirm "Knoten aus Discovery-Ergebnis hinzufügen" öffnet sich und zeigt eine Liste der erkannten Knoten an.

3. Wählen Sie aus der Liste "Erkannte Knoten" die Knoten aus, die Sie hinzufügen möchten, und klicken Sie auf den Pfeil, um sie zur Liste "Zu schützende Knoten" hinzuzufügen. Klicken Sie zum Abschluss auf "Weiter".

   Hinweis: Sie können die Liste nach Knotennamen oder Domäne filtern, um die Liste zu verkürzen.

4. (Optional) Wählen Sie einen oder mehrere Knoten aus und klicken Sie auf "Ausgewählte Knoten verbergen", um Knoten auszublenden, die Sie nicht sichern wollen.

5. (Optional) Aktivieren Sie die Option "Verborgene Knoten anzeigen", um verborgene Knoten wieder auf der Liste "Erkannte Knoten" anzuzeigen. Um die Knoten wieder auszublenden, deaktivieren Sie die Option.

6. Geben Sie im Fenster "Knoten-Anmeldeinformationen" einen Benutzernamen und ein Kennwort für den Knoten an, den Sie hinzufügen wollen. Sie können globale Anmeldeinformationen angeben oder Anmeldeinformationen auf die ausgewählten Knoten anwenden.

7. Klicken Sie auf Fertig stellen.

Die Knoten werden hinzugefügt.

Hinzufügen von Knoten durch Importieren virtueller Rechner aus ESX/VC

Die Option "Knoten hinzufügen" lässt Sie alle virtuellen Rechner auf einem von Ihnen festgelegten ESX- oder vCenter-Serverhost finden und hinzufügen.

Hinweis: Rechner mit installierten VMware-Tools sind die einzigen virtuellen Rechner, die gefunden werden können.

So fügen Sie Knoten durch Importieren virtueller Rechner aus ESX/VC hinzu

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird geöffnet.

2. Klicken Sie in der Symbolleiste "Knoten" auf "Hinzufügen" und dann im Pop-up-Menü auf "Virtuelle Rechner aus ESX/VC importieren".

   Das Dialogfeld "Knoten erkennen" wird geöffnet.

3. Füllen Sie im Dialogfeld "Knoten erkennen" die folgenden Felder aus:

   - ESX Server- oder vCenter-Serverhost: Lässt Sie den Hypervisor festlegen, den Sie durchsuchen wollen.
   - Benutzername
   - Kennwort
   - Port
   - Protokoll

   Klicken Sie auf Verbinden.

   Die Anwendung durchsucht den angegebenen Hypervisor.

4. Klicken Sie auf "Weiter", sobald die Suche beendet ist.

   Das Dialogfeld "Knoten-Anmeldeinformationen" wird angezeigt.

5. Geben Sie im Dialogfeld "Knoten-Anmeldeinformationen" einen globalen Benutzernamen und ein Kennwort für alle erkannten virtuellen Rechner an, und klicken Sie auf "Auf ausgewählte Knoten anwenden".

6. (Optional) Klicken Sie auf einen virtuellen Rechner, um die festgelegten Anmeldeinformationen für den virtuellen Rechner einzugeben.

7. Klicken Sie auf "Fertig stellen".

Die ausgewählten virtuellen Rechner werden zu der Knotengruppe hinzugefügt.

Importieren von Knoten aus einer Datei

CA ARCserve Central Protection Manager lässt Sie mehrere Knoten aus einer Datei importieren. Sie können Knoten aus einer Datei mit durch Komma getrennten Werten (.txt) oder einer Tabelle (.CSV) importieren.

So importieren Sie Knoten aus einer Datei

1. Melden Sie sich bei der Anwendung an.

   Wählen Sie in der Navigationsleiste auf der Startseite "Knoten" aus.

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Symbolleiste "Knoten" auf "Hinzufügen" und dann im Pop-up-Menü auf "Knoten aus Datei importieren".

   Das Dialogfeld "Knoten auswählen" wird geöffnet.

3. Klicken Sie auf "Durchsuchen", um die Datei festzulegen, die die Knoten enthält, die Sie importieren wollen.

   Hinweis: Sie können eine Datei mit durch Komma getrennten Werten (CSV) oder eine Textdatei, die durch Komma getrennte Werte enthält, festlegen.

   Klicken Sie auf "Hochladen".

   Die Knotennamen und die entsprechenden Benutzernamen werden auf dem Dialogfeld angezeigt.

4. Klicken Sie auf "Weiter".

   Das Dialogfeld "Knoten-Anmeldeinformationen" wird angezeigt.

   Wenn die Benutzernamen und angegebene Kennwörter richtig sind, wird im Feld "Bestätigt" ein grünes Häkchen angezeigt. Wenn die Benutzernamen und angegebene Kennwörter nicht richtig sind, wird im Feld "Bestätigt" ein rotes Ausrufezeichen angezeigt.

5. Wählen Sie eine der folgenden Vorgehensweisen:

   - Um die Knoten hinzuzufügen, überprüfen Sie, dass alle Benutzernamen und Kennwörter richtig sind. Um die Anmeldeinformationen für einen bestimmten Knoten zu ändern, klicken Sie auf das Feld "Knotennamen".

     Das Dialogfeld "Anmeldeinformationen validieren" öffnet sich.

     Füllen Sie im Dialogfeld "Anmeldeinformationen validieren" die erforderlichen Felder aus und klicken Sie auf "OK".

   - Um einen globalen Benutzernamen und ein Kennwort auf alle Knoten anzuwenden, füllen Sie die Felder für "Benutzernamen" und "Kennwort" aus und klicken Sie auf "Auf ausgewählte Knoten anwenden".

Der globale Benutzername und das Kennwort werden auf alle Knoten angewendet.

Klicken Sie auf Fertig stellen.

Die Knoten werden hinzugefügt.

Aktualisieren von Knoten

CA ARCserve Central Protection Manager lässt Sie Informationen über Knoten aktualisieren, die zuvor hinzugefügt wurden. Sie aktualisieren Knoten, wenn die folgenden Bedingungen entstehen:

- **Alle Knoten:**
  - Ein neues Produkt wurde auf dem Knoten installiert, nachdem der Knoten mit CA ARCserve Central Protection Manager registriert wurde.
  - Der Benutzername oder das Kennwort für den Knoten wurden aktualisiert, nachdem der Knoten mit CA ARCserve Central Protection Manager registriert wurde.
- **CA ARCserve Backup-Knoten:**
  - Ein CA ARCserve Backup-Zweigstellenserver wurde auf einem CA ARCserve Backup-Primärserver aktualisiert.
  - Ein zentraler CA ARCserve Backup-Primärserver wurde auf einem CA ARCserve Backup-Primärserver aktualisiert, nachdem der zentrale Primärserver mit CA ARCserve Central Protection Manager registriert wurde.

  Hinweis: Wenn Sie Knoten hinzufügen oder aktualisieren, die als CA ARCserve Backup-Zweigstellenserver fungieren und einem primären Zentralserver zugeordnet sind, wird der Hostname des primären Zentralservers in zwei Speicherorten auf dem Fenster "Knoten" angezeigt. Der erste Speicherort auf dem Fenster "Knoten" ist die Gruppe "Alle Knoten". Der vollständige Name des Servers wird in der Gruppe "Alle Knoten" angezeigt, ungeachtet der Zeichenlänge des Hostnamens des Servers. Der zweite Speicherort auf dem Fenster "Knoten" ist "Globale Dashboard-Gruppen". Wenn der Hostname des Servers mehr als 15 Zeichen enthält, wird der Hostname des Servers in "Globale Dashboard-Gruppen" auf 15 Zeichen verkürzt.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Wählen Sie in der Navigationsleiste auf der Startseite "Knoten" aus.

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Menüleiste "Gruppen" auf die Gruppe "Alle Knoten" oder klicken Sie auf den Gruppennamen, der die Knoten enthält, die Sie aktualisieren wollen.

   Die der Gruppe zugeordneten Knoten werden in der Knotenliste angezeigt.

3. Klicken Sie auf die Knoten, die Sie aktualisieren möchten, und klicken Sie anschließend mit der rechten Maustaste, und wählen Sie im Pop-up-Menü die Option "Knoten aktualisieren".

   Das Dialogfeld "Knoten aktualisieren" wird geöffnet.

   Hinweis: Um alle Knoten in der Knotengruppe zu aktualisieren, klicken Sie mit der rechten Maustaste auf den Namen "Knotengruppe", und klicken Sie anschließend im Pop-up-Menü auf "Knoten aktualisieren".

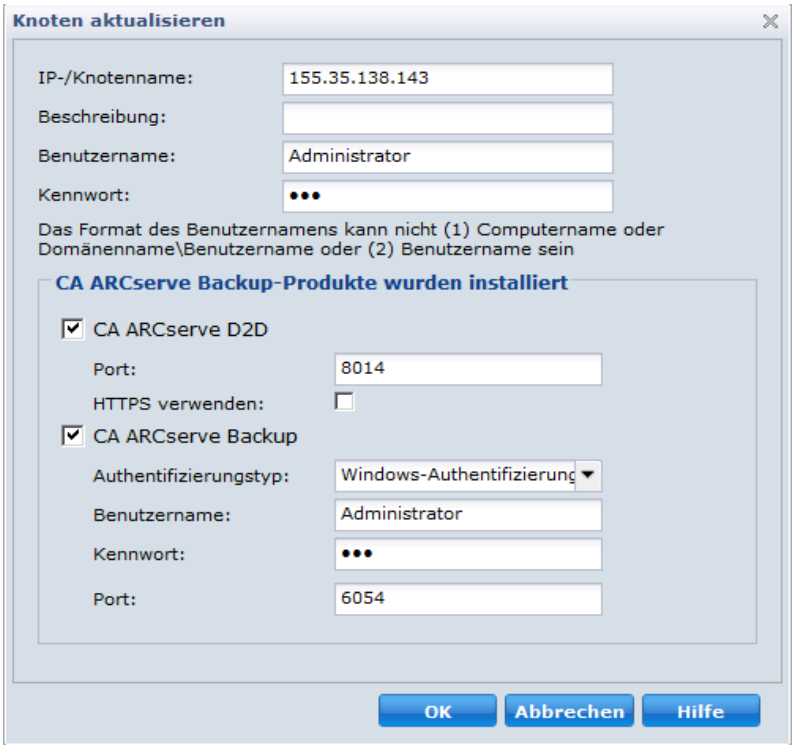
4. Aktualisieren Sie die Knotendetails nach Bedarf.

   Hinweis: Um mehrere Knoten mit der rechten Maustaste auf der Knotenliste zu aktualisieren, wählen Sie die gewünschten Knoten aus, klicken Sie mit der rechten Maustaste auf einen Knoten, und klicken Sie dann im Pop-up-Menü auf "Aktualisieren". Benutzername und Kennwort sind für alle ausgewählten Knoten gleich. Standardmäßig sind die Option "Neue Anmeldeinformationen angeben" und das Kontrollkästchen "Steuerung übernehmen für Knoten" aktiviert. Sie können einen neuen Benutzernamen und Kennwort für die ausgewählten Knoten angeben und können diesen Server zwingen, die Knoten zu verwalten. Außerdem können Sie die Option "Vorhandene Anmeldeinformationen verwenden", um den aktuellen Benutzernamen und das aktuelle Kennwort anzuwenden. Die Felder werden deaktiviert.

5. Klicken Sie auf "OK".

   Das Dialogfeld "Knoten aktualisieren" wird geschlossen, und die Knoten werden aktualisiert.

   Hinweis: Wenn Sie mindestens einen der im nächsten Schritt beschriebenen Felder aktualisieren, wird das Dialogfeld "Knoten aktualisieren" geöffnet, in dem Sie mehr Details angeben können.



6. (Optional) Wenn die aktualisierten Informationen nicht in der Knotenliste anzeigt werden, klicken Sie in der Symbolleiste auf "Aktualisieren".

Der Knoten wird aktualisiert.

Löschen von Knoten

CA ARCserve Central Protection Manager lässt Sie Knoten aus Ihrer Umgebung löschen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie in der Menüleiste "Gruppen" auf die Gruppe "Alle Knoten" oder klicken Sie auf den Gruppennamen, der den Knoten enthält, den Sie löschen wollen.

   Die der Gruppe zugeordneten Knoten werden in der Knotenliste angezeigt.

3. Markieren Sie einen oder mehrere Knoten, die Sie löschen wollen, und klicken Sie dann in der Symbolleiste auf "Löschen".

   Eine Bestätigungsmeldung wird angezeigt.

4. Wählen Sie eine der folgenden Vorgehensweisen:

   - Klicken Sie auf "Ja", um den Knoten zu löschen.

   Klicken Sie auf "Nein", wenn Sie den Knoten nicht löschen wollen.

Exportieren von Knoten in eine Datei

CA ARCserve Central Protection Manager lässt Sie die Knoten aus der ausgewählten Knotengruppe mit Anmeldeinformationen in eine CSV-Datei exportieren.

So exportieren Sie Knoten in eine Datei

1. Melden Sie sich bei der Anwendung an.

   Wählen Sie in der Navigationsleiste auf der Startseite "Knoten" aus.

   Der Bildschirm "Knoten" wird angezeigt.

2. Wählen Sie eine Knotengruppe für den Export aus.

   Die Knoten für die ausgewählte Knotengruppe werden angezeigt.

3. Klicken Sie in der Knoten-Symbolleiste auf "Exportieren".

   Eine Meldung wird angezeigt, die Sie informiert, dass die CSV-Datei Kennwörter enthält, die in einfachem Text angezeigt werden.

   Klicken Sie auf "Ja", um die CSV-Datei zu öffnen oder zu speichern, oder auf "Nein", um den Vorgang abzubrechen.

Die Konten werden in eine CSV-Datei exportiert.

Anmelden bei CA ARCserve D2D-Knoten

Auf der CA ARCserve Central Protection Manager-Startseite der Anwendung können Sie sich bei CA ARCserve D2D-Knoten anmelden.

So melden Sie sich bei CA ARCserve D2D-Knoten an

1. Öffnen Sie die Anwendung und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Suchen und klicken Sie auf den Knoten, auf dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   Hinweis: Wenn sich ein neues Browser-Fenster nicht öffnet, stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser alle Pop-up-Fenster oder Pop-up-Fenster nur auf dieser Website zulassen.

Sie sind beim CA ARCserve D2D-Knoten angemeldet.

Hinweis: Wenn Sie sich das erste Mal beim CA ARCserve D2D-Knoten anmelden, wird möglicherweise eine HTML-Seite geöffnet, die eine Warnmeldung anzeigt. Dies kann bei Verwendung von Internet Explorer auftreten. Um dieses Problem zu lösen, schließen Sie Internet Explorer und wiederholen Sie die Schritt 3. Danach sollten Sie sich problemlos beim CA ARCserve D2D-Knoten anmelden können.

Aktualisieren von Knoten und Richtlinien nach einer Änderung des Hostnamens des CA ARCserve Central Applications-Servers

Wenn Sie den Hostnamen des CA ARCserve Central Protection Manager-Servers geändert haben, aktualisieren Sie die Knoten und die Richtlinien, die auf die Knoten angewendet werden. Sie führen diese Aufgaben aus, um die Beziehung zwischen dem CA ARCserve Central Protection Manager-Server und den Knoten, die der CA ARCserve Central Protection Manager-Server schützt, zu verwalten. In der folgenden Tabelle sind die möglichen Szenarien sowie die entsprechenden Korrekturmaßnahmen beschrieben.

Szenario	Korrekturmaßnahme
Der Knoten wurde hinzugefügt, nachdem der Hostname des CA ARCserve Central Protection Manager-Servers geändert wurde.	Es ist keine Aktion erforderlich.
Der Knoten wurde hinzugefügt, bevor der Hostname des CA ARCserve Central Protection Manager-Servers geändert wurde, und eine Richtlinie wurde nicht auf den Knoten angewandt.	Aktualisieren Sie den Knoten. Weitere Informationen finden Sie unter Aktualisieren von Knoten (siehe Seite 66).
Der Knoten wurde hinzugefügt, bevor der Hostname des CA ARCserve Central Protection Manager-Servers geändert wurde, und eine Richtlinie wurde auf den Knoten angewandt.	Wenden Sie die Richtlinie erneut an. Weitere Informationen finden Sie unter Bereitstellen von Richtlinien (siehe Seite 139).

Zusammenführungsjob-Optionen

CA ARCserve Central Protection Manager lässt Sie Zusammenführungsjobs für jeden Knoten unterbrechen und jederzeit wiederaufnehmen. Der Prozess des Unterbrechens und Wiederaufnehmens von Zusammenführungsjobs wirkt sich nicht auf Jobs aus, die sich in Bearbeitung befinden.

Zusammenführungsjob auf einem Knoten unterbrechen

CA ARCserve Central Protection Manager lässt Sie einen Zusammenführungsjob auf einem bestimmten Knoten unterbrechen.

Zum Beispiel können Zusammenführungsjobs Systemressourcen verbrauchen und verursachen, dass Sicherungsjobs verlangsamt ausgeführt werden. Verwenden Sie die Unterbrechungsoption, um einen sich in Bearbeitung befindlichen Zusammenführungsjob anzuhalten, sodass sich in Bearbeitung befindliche Sicherungsjobs mit höchstmöglicher Effizienz abschließen können. Nachdem die Sicherungen abgeschlossen haben, können Sie den Zusammenführungsjob wiederaufnehmen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite von CA ARCserve Central Protection Manager in der Navigationsleiste auf "Knoten", um das Fenster "Knoten" zu öffnen.
2. Wählen Sie die Knotengruppe aus, die die Knoten mit den Zusammenführungsjobs enthält, die Sie unterbrechen wollen.

   Eine Liste von Knoten für die ausgewählte Knotengruppe wird angezeigt.
3. Klicken Sie auf die Knoten mit den Zusammenführungsjobs, die Sie unterbrechen wollen. Klicken Sie dann mit der rechten Maustaste auf die ausgewählten Knoten und im Pop-up-Menü auf "Zusammenführungsjob unterbrechen".

   Hinweis: Standardmäßig ist die Option "Zusammenführungsjob unterbrechen" deaktiviert. Wenn der Knoten derzeit einen Zusammenführungsjob ausführt, wie in der Job-Spalte angezeigt, wird die Option "Zusammenführungsjob unterbrechen" aktiviert.

Der Zusammenführungsjob des ausgewählten Knotens wird unterbrochen und kann auf der CA ARCserve D2D-Startseite überprüft werden.

Zusammenführungsjob auf einem Knoten wiederaufnehmen

CA ARCserve Central Protection Manager lässt Sie Zusammenführungsjobs wieder aufnehmen, die für bestimmte Knoten unterbrochen wurden.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite von CA ARCserve Central Protection Manager in der Navigationsleiste auf "Knoten", um das Fenster "Knoten" zu öffnen.
2. Wählen Sie die Knotengruppe aus, die die Knoten mit den Zusammenführungsjobs enthält, die Sie wiederaufnehmen wollen.

   Eine Liste von Knoten für die ausgewählte Knotengruppe wird angezeigt.
3. Klicken Sie auf die Knoten mit den Zusammenführungsjobs, die unterbrochen sind, und die Sie nun wiederaufnehmen wollen. Klicken Sie dann mit der rechten Maustaste auf die ausgewählten Knoten und im Pop-up-Menü auf "Zusammenführungsjob wieder aufnehmen".

   Hinweis: Die Option "Zusammenführungsjob wieder aufnehmen" wird aktiviert, wenn kein Sicherungsjob ausgeführt wird und die Zusammenführungsjobs unterbrochen sind.

Der Zusammenführungsjob des ausgewählten Knotens wird wieder aufgenommen und kann auf der CA ARCserve D2D-Startseite überprüft werden.

Synchronisationsdaten und -optionen

CA ARCserve Central Protection Manager ermöglicht die Synchronisation der Daten für jeden Knoten durch das Senden von Informationen vom CA ARCserve Backup-Primärserver (asdb), CA ARCserve D2D, oder der zentralen Global Dashboard-Primärdatenbank (central_asdb) an die CA ARCserve Central Protection Manager-Datenbank (ARCAppDB).

Beim Synchronisieren werden die Daten in den unterschiedlichen Datenbanken vereinheitlicht und aktualisiert, sodass die Datenbank des zentralen Servers dieselben Informationen wie die Datenbanken der einzelnen registrierten Zweigstellenserver enthält.

Dieser Abschnitt enthält folgende Themen:

Durchführen einer vollständigen Synchronisation von CA ARCserve Backup-Daten für einen bestimmten Knoten oder eine Knotengruppe (siehe Seite 73)
Durchführen einer inkrementellen Synchronisation von CA ARCserve Backup-Daten für einen bestimmten Knoten oder eine bestimmte Knotengruppe (siehe Seite 73)
Durchführen einer vollständigen Synchronisation von CA ARCserve D2D-Daten für einen bestimmten Knoten oder eine Knotengruppe (siehe Seite 74)

Durchführen einer vollständigen Synchronisation von CA ARCserve Backup-Daten für einen bestimmten Knoten oder eine Knotengruppe

CA ARCserve Central Protection Manager lässt Sie eine vollständige Synchronisation von CA ARCserve Backup-Daten auf einem bestimmten Knoten oder einer bestimmten Knotengruppe ausführen.

Während eines vollständigen CA ARCserve Backup-Synchronisationsvorgangs wird der CA ARCserve Backup-Datenbankprozess einige Minuten lang angehalten. Dieses Verhalten kann die Protokollierung von CA ARCserve Backup-Jobinformationen verhindern, bis der Datenbanksynchronisationsprozess vollständig ist.

So führen Sie eine vollständige Synchronisation von CA ARCserve Backup-Daten für einen bestimmten Knoten oder eine bestimmte Knotengruppe durch

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Wählen Sie die Knotengruppe aus, die die Knoten enthält, die Sie synchronisieren wollen.

   Eine Liste von Knoten für die ausgewählte Knotengruppe wird angezeigt.

3. Wählen Sie eine der folgenden Vorgehensweisen:

   - Wählen Sie für einen bestimmten Knoten den CA ARCserve Backup-Knoten auf der rechten Seite der "Gruppen" aus und klicken Sie im Kontextmenü auf "Vollständige Synchronisation für CA ARCserve Backup" oder auf die Schaltfläche "Synchronisationsdaten" in der Symbolleiste "Knoten".
   - Klicken Sie für eine Knotengruppe mit der rechten Maustaste auf die Knotengruppe und im Pop-up-Menü auf "Vollständige Synchronisation mithilfe von CA ARCserve Backup".

CA ARCserve Central Protection Manager übergibt eine vollständige Synchronisation von CA ARCserve Backup-Daten für den ausgewählten Knoten oder die ausgewählte Knotengruppe.

Durchführen einer inkrementellen Synchronisation von CA ARCserve Backup-Daten für einen bestimmten Knoten oder eine bestimmte Knotengruppe

CA ARCserve Central Protection Manager lässt Sie eine inkrementelle Synchronisation von CA ARCserve Backup-Daten auf einem bestimmten Knoten ausführen.

"Inkrementelle Synchronisation mithilfe von CA ARCserve Backup" synchronisiert Daten, die geändert, gelöscht oder hinzugefügt wurden, nachdem die letzte Synchronisation durchgeführt wurde. Die synchronisierten Daten werden komprimiert, um die Größe vor der Datenübertragung zu minimieren.

So führen Sie eine inkrementelle Synchronisation von CA ARCserve Backup-Daten für einen bestimmten Knoten oder eine bestimmte Knotengruppe durch

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Wählen Sie die Knotengruppe aus, die die Knoten enthält, die Sie synchronisieren wollen.

   Eine Liste von Knoten für die ausgewählte Knotengruppe wird angezeigt.

3. Wählen Sie eine der folgenden Vorgehensweisen:

   - Wählen Sie für einen bestimmten Knoten den CA ARCserve Backup-Knoten auf der rechten Seite der "Gruppen" aus und klicken Sie im Kontextmenü auf "Inkrementelle Synchronisation für CA ARCserve Backup" oder auf die Schaltfläche "Synchronisationsdaten" in der Symbolleiste "Knoten".
   - Klicken Sie für eine Knotengruppe mit der rechten Maustaste auf die Knotengruppe und im Pop-up-Menü auf "Inkrementelle Synchronisation mithilfe von CA ARCserve Backup".

CA ARCserve Central Protection Manager übergibt eine inkrementelle Synchronisation von CA ARCserve Backup-Daten für den ausgewählten Knoten oder die ausgewählte Knotengruppe.

Durchführen einer vollständigen Synchronisation von CA ARCserve D2D-Daten für einen bestimmten Knoten oder eine Knotengruppe

CA ARCserve Central Protection Manager lässt Sie eine vollständige Synchronisation von CA ARCserve D2D-Daten auf einem bestimmten Knoten oder einer bestimmten Knotengruppe ausführen.

So führen Sie eine vollständige Synchronisation von CA ARCserve D2D-Daten für einen bestimmten Knoten oder eine bestimmte Knotengruppe durch

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Wählen Sie die Knotengruppe aus, die die Knoten enthält, die Sie synchronisieren wollen.

Eine Liste von Knoten für die ausgewählte Knotengruppe wird angezeigt.

3. Wählen Sie eine der folgenden Vorgehensweisen:

   - Wählen Sie für einen bestimmten Knoten den CA ARCserve D2D-Knoten auf der rechten Seite der "Gruppen" aus und klicken Sie im Kontextmenü auf "Vollständige Synchronisation für CA ARCserve D2D" oder auf die Schaltfläche "Synchronisationsdaten" in der Symbolleiste "Knoten".
   - Klicken Sie für eine Knotengruppe mit der rechten Maustaste auf die Knotengruppe und im Pop-up-Menü auf "Vollständige Synchronisation mithilfe von CA ARCserve D2D".

CA ARCserve Central Protection Manager übergibt eine vollständige Synchronisation von CA ARCserve D2D-Daten für den ausgewählten Knoten oder die ausgewählte Knotengruppe.

Knoteneinstellungen

CA ARCserve Central Protection Manager lässt Sie einen lokalen Ablaufplan für jeden CA ARCserve Backup- oder zentralen Global Dashboard-Primärknoten einrichten, um inkrementelle Synchronisation auszuführen.

Anwenden von CA ARCserve Backup-Datensynchronisations-Ablaufplänen

Die CA ARCserve Backup-Einstellung lässt Sie an jeden CA ARCserve Backup-Knoten angepasste Ablaufpläne festlegen.

So wenden Sie CA ARCserve Backup-Datensynchronisations-Ablaufpläne an

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Knoten".

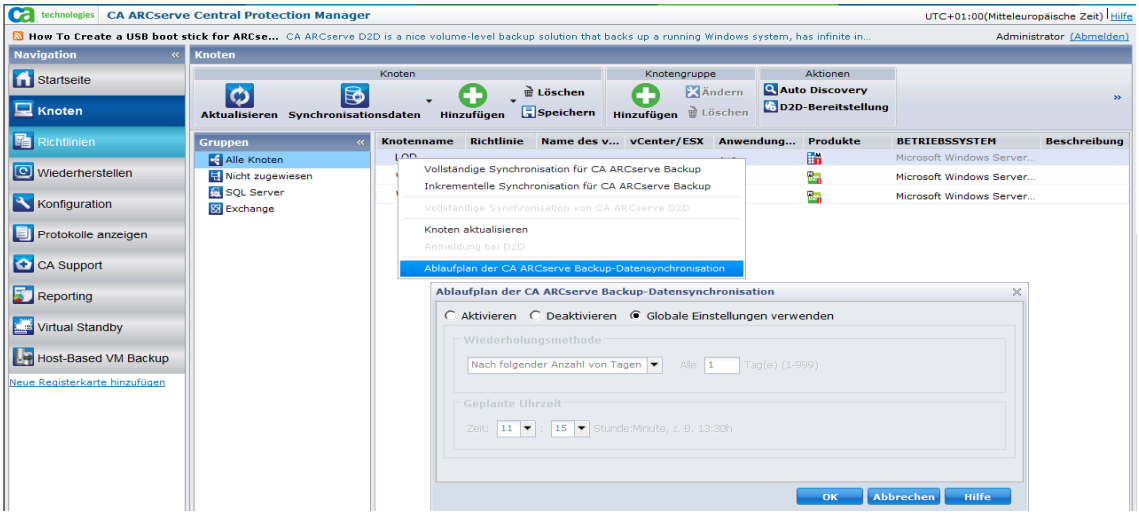
   Der Bildschirm "Knoten" wird angezeigt.

2. Wählen Sie die Knotengruppe aus der Gruppenliste mit dem Knoten aus, auf den Sie die CA ARCserve Backup-Einstellung anwenden möchten.

   Eine Liste von Knoten für die ausgewählte Knotengruppe wird angezeigt.

3. Wählen Sie den Knoten aus, um die Einstellung anzuwenden und klicken Sie dann im Kontextmenü auf "Ablaufplan der CA ARCserve Backup-Datensynchronisation".

   Das Dialogfeld "Ablaufplan der CA ARCserve Backup-Datensynchronisation" wird geöffnet.



4. Wählen Sie eine der folgenden Optionen:

   - **Aktivieren:** Ermöglicht es Ihnen, Ablaufplanoptionen durch das Eingeben einer Wiederholungsmethode und einer geplanten Zeit festzulegen:
     - Nach folgender Anzahl von Tagen
     - Alle ausgewählten Tage der Woche
     - Alle ausgewählten Tage des Monats
   - **Deaktivieren:** Mit dieser Option, werden keine Einstellungen angewendet.
   - **Globale Einstellungen verwenden:** Ermöglicht es Ihnen, die im CA ARCserve Backup-Konfigurationsmodul konfigurierten gobalen Einstellungen anzuwenden. Weitere Details finden Sie unter Ablaufpläne der CA ARCserve Backup-Datensynchronisation.

5. Klicken Sie auf "OK".

Die CA ARCserve Backup-Einstellungen werden angewendet.

Funktionen für Knotengruppen

CA ARCserve Central Protection Manager lässt Sie Knotengruppen erstellen, die jeder Gruppe individuelle Knoten zuweisen, sowie Knotengruppen ändern und löschen können.

Hinweis: Sie können nur die Knotengruppen ändern und löschen, die Sie erstellt haben.

Hinzufügen von Knotengruppen

Knotengruppen lassen Sie eine Sammlung von auf eine Gemeinsamkeit basierenden CA ARCserve D2D-Quellcomputern verwalten. Zum Beispiel können Sie Knotengruppen definieren, die nach der Abteilung klassifiziert sind, die sie unterstützen: Buchhaltung, Marketing, Recht, Personal, und so weiter.

Die Anwendung enthält die folgenden Knotengruppen:

- **Standardgruppen:**
  - **Alle Knoten--**Enthält alle der Anwendung zugeordneten Knoten.
  - **Knoten ohne Gruppe** -- Enthält alle mit der Anwendung verknüpften Knoten, die keiner Knotengruppe zugewiesen sind.
  - **Knoten ohne Richtlinie** -- Enthält alle mit der Anwendung verknüpften Knoten, denen keine Richtlinie zugewiesen ist.
  - **SQL Server:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft SQL Server ist auf dem Knoten installiert.
  - **Exchange:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft Exchange Server ist auf dem Knoten installiert.

  Hinweis: Sie können die Standardknotengruppen nicht ändern oder löschen.
- **Benutzerdefinierte Gruppen:** Enthält benutzerdefinierte Knotengruppen.
- **vCenter/ESX-Gruppen:** Wenn Sie einen Knoten aus der Option "Virtuelle Rechner aus vCenter/ESX importieren" hinzufügen, wird der Name des vCenter/ESX-Servers zu dieser Gruppe hinzugefügt.
- **Globale Dashboard-Gruppe:** Enthält alle dem zentralen Primärserver zugeordneten Knoten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste der Startseite auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie in der Symbolleiste "Knotengruppe" auf "Hinzufügen".

   Das Dialogfeld "Gruppe hinzufügen" öffnet sich und die Knoten werden in der Liste der verfügbaren Knoten angezeigt.

3. Geben Sie einen Gruppennamen für die Knotengruppe an.
4. Geben Sie im Dialogfeld "Gruppe hinzufügen" folgende Felder an:
   - **Gruppe:** Wählen Sie den Gruppennamen aus, der die Knoten enthält, die Sie zuweisen möchten.
   - **Knotennamenfilter:** Lässt Sie die verfügbaren Knoten basierend auf einer Gemeinsamkeit filtern.

     Hinweis: Das Feld "Knotenname" unterstützt die Verwendung von Platzhalterzeichen.

     Acc* lässt Sie beispielsweise alle Knoten filtern, die einen Knotennamen haben, der mit "Acc." beginnt. Um die Filterergebnisse zu löschen, klicken Sie im Feld "Filter" auf X.
5. Um Knoten zur Knotengruppe hinzuzufügen, wählen Sie die Knoten aus, die Sie hinzufügen möchten, und klicken Sie auf den einzelnen Rechtspfeil.

   Die Knoten verschieben sich von der Liste "Verfügbare Knoten" zur Liste "Ausgewählte Knoten" und werden der Knotengruppe zugewiesen.

   Hinweis: Um alle Knoten auszuwählen und aus der aktuellen Gruppe zu verschieben, klicken Sie auf den doppelten Rechtspfeil.
6. (Optional) Um Knoten von der Liste "Ausgewählte Knoten" in die Liste "Verfügbare Knoten" zu verschieben, klicken Sie auf den einzelnen Linkspfeil.

   Hinweis: Um alle Knoten auszuwählen und in der aktuellen Gruppe zu verschieben, klicken Sie auf den doppelten Linkspfeil.
7. Klicken Sie auf "OK".

Die Knotengruppe wird hinzugefügt.

Ändern von Knotengruppen

Die Anwendung lässt Sie die Knotengruppen ändern, die Sie erstellt haben. Sie können Knoten zu Knotengruppen hinzufügen und aus ihnen entfernen und den Namen von Knotengruppen ändern.

Hinweis: Sie können folgende Knotengruppen nicht ändern:

- **Alle Knoten--**Enthält alle der Anwendung zugeordneten Knoten.
- **Knoten ohne Gruppe** -- Enthält alle mit der Anwendung verknüpften Knoten, die keiner Knotengruppe zugewiesen sind.
- **Knoten ohne Richtlinie** -- Enthält alle mit der Anwendung verknüpften Knoten, denen keine Richtlinie zugewiesen ist.
- **SQL Server:** Enthält alle der Anwendung zugeordneten Knoten und Microsoft SQL Server ist installiert.
- **Exchange:** Enthält alle der Anwendung zugeordneten Knoten und Microsoft SQL Server ist installiert.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie auf die Knotengruppe, die Sie ändern wollen, und dann in der Symbolleiste der Knotengruppe auf "Ändern".

   Das Dialogfeld "Gruppe ändern" wird geöffnet.

3. Um den Gruppennamen zu ändern, geben Sie einen neuen Namen im Feld "Gruppennamen" an.

4. Um Knoten zur Knotengruppe hinzuzufügen, wählen Sie die Knoten aus, die Sie zur Knotengruppe hinzufügen möchten, und klicken Sie auf den Rechtspfeil.

   Die Knoten verschieben sich von der Liste "Verfügbare Knoten" zur Liste "Ausgewählte Knoten" und werden der Knotengruppe zugewiesen.

   Hinweis: Um alle Knoten von der Liste "Verfügbare Knoten" zur Liste "Ausgewählte Knoten" zu verschieben, klicken Sie auf den doppelten Rechtspfeil.

5. Um Knoten aus der Knotengruppe zu entfernen, klicken Sie auf den linken Pfeil, um einen, oder auf den doppelten Linkspfeil, um alle Knoten zu entfernen.

6. (Optional) Um die verfügbaren Knoten basierend auf einer Gemeinsamkeit zu filtern, legen Sie im Feld "Knotennamenfilter" einen Filterwert fest.

   Hinweis: Das Feld "Filter" unterstützt die Verwendung von Platzhalterzeichen.

   Acc* lässt Sie beispielsweise alle Knoten filtern, die einen Knotennamen haben, der mit "Acc." beginnt. Um die Filterergebnisse zu löschen, klicken Sie im Feld "Filter" auf X.

7. Klicken Sie auf "OK".

Die Knotengruppe wird geändert.

Hinweis: Wenn Sie einen Global Dashboard-Knoten aus CA ARCserve Backup zu einer Knotengruppe zuweisen, werden alle CA ARCserve Backup-Zweigstellen im CA ARCserve Backup-Global Dashboard-Knoten abgezeigt, auch wenn sie nicht zur Knotengruppe gehören. Wenn Sie die Knotengruppe auswählen, die den CA ARCserve Backup-Global Dashboard-Knoten in der CA ARCserve Central Reporting-Anwendung enthält, enthalten die Berichte infolgedessen nicht für alle Zweigstellen des Global Dashboard-Knotens Daten.

Löschen von Knotengruppen

Sie können eine Knotengruppe nach Bedarf löschen. Wenn Sie eine manuell hinzugefügte Gruppe löschen, werden die virtuellen Rechner nicht aus der Anwendung entfernt. Wenn Sie allerdings eine Gruppe löschen, die mit einer ESX- oder vCenter Server-Discovery automatisch erstellt wurde, werden die Gruppe und alle virtuellen Rechner aus der Anwendung gelöscht.

Die Anwendung lässt Sie die Knotengruppen löschen, die Sie erstellt haben.

Sie können folgende Knotengruppen nicht löschen:

- **Alle Knoten--**Enthält alle der Anwendung zugeordneten Knoten.
- **Knoten ohne Gruppe** -- Enthält alle mit der Anwendung verknüpften Knoten, die keiner Knotengruppe zugewiesen sind.
- **Knoten ohne Richtlinie** -- Enthält alle mit der Anwendung verknüpften Knoten, denen keine Richtlinie zugewiesen ist.
- **SQL Server:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft SQL Server ist auf dem Knoten installiert.
- **Exchange:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft Exchange Server ist auf dem Knoten installiert.

Hinweis: Das Löschen von Knotengruppen löscht keine individuelle Knoten aus der Anwendung.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste der Startseite auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie auf die Knotengruppe, die Sie löschen wollen, und dann in der Symbolleiste der Knotengruppe auf "Löschen".

   Das Meldungsdialogfeld "Bestätigen" öffnet sich.

3. Wenn Sie sicher sind, dass Sie die Knotengruppe löschen möchten, klicken Sie auf "Ja".

   Hinweis: Klicken Sie auf "Nein", wenn Sie die Knotengruppe nicht löschen wollen.

Die Knotengruppe wird gelöscht.

Mithilfe von Discovery nach Knoten suchen

CA ARCserve Central Protection Manager lässt Sie mithilfe von Discovery nach Knoten suchen. Protection Manager sucht auf der Basis von Informationen, die im Active Directory eines Servers aufgewahrt werden, nach Knoten. Active Directory bietet folgende Informationen:

- Rechnername
- Betriebssysteminformationen (Name, Version, Patch)
- wenn Microsoft Exchange Server auf dem Rechner vorhanden ist
- wenn Microsoft SQL Server auf dem Rechner vorhanden ist

So suchen Sie mithilfe von Discovery nach Knoten

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Kategorie "Knoten" auf "Erkennen", um das Dialogfeld "Knoten durch Active Directory erkennen" zu öffnen.

3. Vervollständigen Sie folgende Felder im Dialogfeld "Discovery nach Active Directory" und klicken Sie auf "Hinzufügen":

   - (Domäne) Benutzername
   - (Domäne) Kennwort
   - Computernamenfilter

   Klicken Sie auf "Erkennen".

   Der Discovery-Vorgang (siehe Seite 61) beginnt.

4. Wenn der Discovery-Vorgang abgeschlossen ist, wird folgende Bestätigungsmeldung angezeigt:

   `Möchten Sie weitere Knoten aus dem Discovery-Ergebnis hinzufügen?`

   Wählen Sie eine der folgenden Vorgehensweisen:

   - Klicken Sie auf "Ja", um zu "Knoten aus Discovery-Ergebnis hinzufügen" zu gelangen.
   - Klicken Sie auf "Nein", um das Meldungsfenster zu schließen.

   Hinweis: Wenn Sie "Ja" auswählen, gehen Sie für weitere Details zur Option "Knoten durch Directory erkennen" (siehe Seite 60).

CA ARCserve D2D-Bereitstellungsaufgaben

Mit CA ARCserve Central Protection Manager können Sie einen oder mehrere Knoten gleichzeitig auf den Zielsystemen per Remote-Zugriff oder lokal bereitstellen. Außerdem können Sie Knoten für die Bereitstellung hinzufügen, bearbeiten oder sie aus der Bereitstellung löschen.

Dieser Abschnitt enthält folgende Themen:

Bereitstellen von CA ARCserve D2D auf Knoten (siehe Seite 84)
Knoten zur Bereitstellung hinzufügen (siehe Seite 85)
Knoten für die Bereitstellung bearbeiten (siehe Seite 86)
Knoten von Bereitstellung löschen (siehe Seite 86)

Bereitstellen von CA ARCserve D2D auf Knoten

CA ARCserve Central Protection Manager lässt Sie die aktuelle Version von CA ARCserve D2D auf einem oder mehreren neuen oder vorhandenen Knoten erkennen und bereitstellen.

Hinweis: Um CA ARCserve D2D auf Computern mit Windows XP bereitzustellen, deaktivieren Sie auf dem Remote-Computer mit Windows XP die Option "Einfache Dateifreigabe verwenden".

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".
2. Klicken Sie in der Ansicht "Knoten" in der Symbolleiste auf "Bereitstellen".

   Das Dialogfeld "Lizenzvereinbarung" wird geöffnet.
3. Lesen und akzeptieren Sie die Bedingungen der Lizenzvereinbarung, und klicken Sie auf "Weiter", um das Dialogfeld "D2D-Bereitstellung" zu öffnen.
4. Geben Sie im Dialogfeld "D2D-Bereitstellung" den Filter "Gruppe" und "Knotenname" für die verfügbaren Knoten an, die auf gemeinsamen Kriterien basieren.

   Name, Version und Status für jeden Knoten werden angezeigt.

   Hinweis: Die Spalte "Version" zeigt die aktuelle D2D-Version an, die auf dem Knoten ausgeführt wird.
5. Klicken Sie auf die Kontrollkästchen neben den Knoten oder klicken Sie auf "Alle auswählen", um alle Knoten anzuzeigen, die zur Bereitstellung auf D2D aufgelistet sind.

   Hinweis: Wenn Sie auf "Alles markieren" klicken, ändert sich die Option in "Markierung aufheben". Hinweis: Wenn Sie einen Knoten aus der Knotenliste auswählen, können Sie die Knotenfelder über die Registerkarte "Knoteninformationen" bearbeiten.
6. Klicken Sie auf "Jetzt bereitstellen", um die neueste D2D-Version, die auf der Titelleiste angezeigt wird, auf den Knoten bereitzustellen.

   Hinweis: Markieren Sie für den Informations- und Bereitstellungsstatus auf einem bestimmten Knoten den Knoten, und wählen Sie die entsprechende Registerkarte im rechten Bereich aus.

Hinweis: Mit CA ARCserve Central Protection Manager können Sie die aktuelle Version von CA ARCserve D2D installieren, ein Upgrade durchführen oder die neueste Version von CA ARCserve D2D auf niedrigeren Versionen oder Knoten, auf denen kein CA ARCserve D2D installiert ist, mithilfe des D2D-Bereitstellungs-Hilfsprogramms bereitstellen.

Knoten zur Bereitstellung hinzufügen

CA ARCserve Central Protection Manager lässt Sie mehrere Knoten zur Bereitstellung hinzufügen.

So fügen Sie Knoten zur Bereitstellung hinzu

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".
2. Klicken Sie in der Ansicht "Knoten" in der Symbolleiste auf "Bereitstellen".

   Das Dialogfeld "Lizenzvereinbarung" wird geöffnet.
3. Lesen und akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf "Weiter".

   Das Dialogfeld zur D2D-Bereitstellung wird geöffnet.
4. Klicken Sie auf "Hinzufügen" und füllen Sie die folgenden Felder im Dialogfeld "D2D-Bereitstellung" aus:
   - Servername
   - Benutzername
   - Kennwort
   - Port
   - Installationspfad
   - Setup erlauben, den Treiber zu installieren (standardmäßig ausgewählt)
   - Neustart (standardmäßig auf "Ja")

     Wenn der Knoten mit einem erfolgreichen Neustart (Ja) bereitgestellt wird, wird der Knoten der von CA ARCserve Central Applications verwalteten Knotenliste hinzugefügt.

     Wenn der Knoten ohne Neustartoption (Nein) bereitgestellt wird, wird der Knoten zur nicht von CA ARCserve Central Applications verwalteten Knotengruppe hinzugefügt.
   - HTTPS verwenden (standardmäßig auf "Nein")

     Sichere HTTPS-Kommunikation bietet eine höhere Sicherheitsebene als HTTP-Kommunikation. HTTPS ist das empfohlene Kommunikationsprotokoll, wenn Sie in Ihrem Netzwerk vertrauliche Informationen übertragen.

   Hinweis: Sie können die Knoten anzeigen, die Sie unter dem Filter "Alle Knoten" und "Ohne Gruppe" hinzugefügt haben.
5. Klicken Sie auf "OK", um die Knoten hinzuzufügen.

Knoten für die Bereitstellung bearbeiten

CA ARCserve Central Protection Manager lässt Sie Knoten für die Bereitstellung bearbeiten.

So bearbeiten Sie Knoten für die Bereitstellung

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".
2. Klicken Sie in der Ansicht "Knoten" in der Symbolleiste auf "Bereitstellen".

   Das Dialogfeld "Lizenzvereinbarung" wird geöffnet.
3. Lesen und akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf "Weiter".

   Der Bildschirm "D2D-Bereitstellung" wird angezeigt.
4. Wählen Sie den Knoten aus, den Sie für die Bereitstellung bearbeiten wollen und klicken Sie auf "Bearbeiten", um das Dialogfeld "Bearbeiten" zu öffnen.
5. Bearbeiten Sie im Dialogfeld "Bearbeiten" die Daten, die Sie ändern wollen, und klicken Sie auf "OK".

Knoten von Bereitstellung löschen

CA ARCserve Central Protection Manager lässt Sie einen oder mehrere Knoten aus der Bereitstellung löschen.

So löschen Sie Knoten aus der Bereitstellung

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".
2. Klicken Sie in der Ansicht "Knoten" in der Symbolleiste auf "Bereitstellen".

   Das Dialogfeld "Lizenzvereinbarung" wird geöffnet.
3. Lesen und akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf "Weiter".

   Der Bildschirm "D2D-Bereitstellung" wird angezeigt.
4. Wählen Sie einen oder mehrere aus der Bereitstellung zu löschende Knoten aus.
5. Klicken Sie auf "Löschen", um die Knoten aus der D2D-Bereitstellung zu löschen.

Filtern von Knotengruppen

CA ARCserve Central Protection Manager lässt Sie Filter verwenden, um Knoten in einer Gruppe anzuzeigen, auf der eine bestimmte Anwendung installiert ist.
CA ARCserve Central Protection Manager lässt Sie die folgenden Anwendungen filtern:

- CA ARCserve Backup
- CA ARCserve D2D
- Microsoft SQL Server
- Microsoft Exchange Server

So filtern Sie Knotengruppen

1. Melden Sie sich bei CA ARCserve Central Protection Manager an.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt:

2. Wählen Sie aus der Liste "Gruppen" die Gruppe aus, die Sie filtern möchten.

   Hinweis: Sie können alle Standardgruppen ("Alle Knoten", "Nicht zugewiesen", "SQL Server", Exchange) und alle benutzerdefiniert benannten Gruppen filtern.

   Aktivieren Sie in der Symbolleiste "Filter" das Kontrollkästchen neben der Anwendung, die Sie filtern möchten.

Die Knotengruppe wird gefiltert.

Verwalten von CA ARCserve D2D-Richtlinien

CA ARCserve Central Protection Manager stellt verschiedene Tools und Optionen bereit, mit denen Sie CA ARCserve D2D-Richtlinien verwalten können. Dieser Abschnitt enthält Informationen darüber, wie Sie D2D-Richtlinien zu Remote-Servern hinzufügen, sie löschen, ändern, D2D bereitstellen und Richtlinien kopieren können. Sie können zentralisierte Sicherungs- und Wiederherstellungsrichtlinien erstellen, die gleichzeitig an mehrere verwaltete Knoten verteilt werden können.

Einige üblichen Beispiele für zentralisierte Sicherungsrichtlinien sind folgende:

- Ablaufpläne
- Jobs
- Ziele
- Ereignisse
- Einstellungen

Dieser Abschnitt enthält folgende Themen:

Erstellen von Richtlinien (siehe Seite 88)
Bearbeiten oder Kopieren von Richtlinien (siehe Seite 137)
Löschen von Richtlinien (siehe Seite 138)
Bereitstellen von Richtlinien (siehe Seite 139)

Erstellen von Richtlinien

CA ARCserve Central Protection Manager lässt Sie eine oder mehrere Richtlinien erstellen, um sie D2D-Knoten zuzuweisen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite von CA ARCserve Central Protection Manager in der Navigationsleiste auf "Richtlinien", um das Fenster "Richtlinien" zu öffnen.
2. Klicken Sie auf "Neu", um das Dialogfeld "Neue Richtlinie" zu öffnen.
3. Geben Sie den Richtliniennamen ein und füllen Sie die erforderlichen Felder in den Registerkarten Sicherungseinstellungen (siehe Seite 89), Einstellungen der Dateikopie (siehe Seite 105), Wiederherstellungspunkte kopieren (siehe Seite 121) und Voreinstellungen (siehe Seite 125) aus.
4. Klicken Sie auf "Speichern".

Die neue Richtlinie wird gespeichert und Sie werden gefragt, ob Sie die Richtlinie jetzt zu den Knoten zuweisen möchten. Wenn Sie auf "Nein" klicken, wird die neue Richtlinie im Fenster "Richtlinien" anzeigt. Wenn Sie auf "Ja" klicken, öffnet sich das Fenster Zuweisung der Richtlinie durchführen/aufheben (siehe Seite 140).

Verwalten von Sicherungseinstellungen

In den Sicherungseinstellungen können Sie die Quelle und das Ziel Ihrer Sicherung, den Ablaufplan für die einzelnen Sicherungstypen und die Einstellungen und erweiterten Einstellungen für Ihre Sicherungsjobs angeben. Diese Einstellungen können jederzeit vom Bildschirm "Richtlinien" aus geändert werden.

Um die Sicherungseinstellungen zu verwalten, klicken Sie in der Navigationsleiste auf der Startseite auf "Richtlinien" und danach auf "Neu".

Dieser Abschnitt enthält folgende Themen:

Festlegen der Schutzeinstellungen (siehe Seite 89)
Festlegen von Sicherungsablaufplänen (siehe Seite 99)
Festlegen der erweiterten Sicherungseinstellungen (siehe Seite 102)
Festlegen von Einstellungen vor/nach der Sicherung (siehe Seite 105)

Festlegen der Schutzeinstellungen

Mit CA ARCserve Central Protection Manager können Sie die Schutzeinstellungen für die Daten, die Sie sichern möchten, festlegen.

So legen Sie Schutzeinstellungen fest

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" öffnet sich und zeigt die Option "Schutzeinstellungen" der Registerkarte "Sicherungseinstellungen" an.

3. Geben Sie das **Sicherungsziel** an.

   Sie können einen lokalen Pfad (Volume oder Ordner) oder einen freigegebenen Remote-Ordner (oder zugeordnetes Laufwerk) als Sicherungsziel angeben.

   a. Wenn Sie die Sicherung in Ihrem lokalen Pfad (Volume oder Ordner) speichern, darf das ausgewählte Sicherungsziel nicht mit der Sicherungsquelle identisch sein. Wenn Sie die Quelle unabsichtlich in das ausgewählte Ziel aufnehmen, ignoriert der Sicherungsjob diesen Teil der Quelle und nimmt ihn nicht in die Sicherung auf.

Wenn Sie z. B. Ihren gesamten lokalen Computer sichern möchten, der aus den Volumes C, D und E besteht, und Volume E gleichzeitig als Ziel angeben, sichert CA ARCserve D2D nur die Volumes C und D auf Volume E. Die Daten auf Volume E werden nicht gesichert. Wenn Sie alle lokalen Volumes sichern wollen, sollten Sie einen Remote-Zielort auswählen.

Wichtig! Vergewissern Sie sich, dass das ausgewählte Zielvolume keine Systeminformationen enthält, da diese in diesem Fall nicht geschützt (gesichert) werden. Nach einer Bare-Metal-Recovery (BMR) kann Ihr System in diesem Fall nicht wiederhergestellt werden.

Hinweis: Dynamische Datenträger können nicht auf Datenträgerebene wiederhergestellt werden. Wenn Ihre Daten auf einem Volume eines dynamischen Datenträgers gesichert sind, können Sie diesen dynamischen Datenträger während der Bare-Metal-Recovery nicht wiederherstellen.

b. Wenn Sie auf einem freigegebenen Remote-Ordner sichern möchten, müssen Sie unbedingt den Pfad des Speicherorts angeben oder den Speicherort suchen und die Benutzeranmeldeinformationen (Benutzername und Kennwort) angeben, um auf den Remote-Computer zuzugreifen.

c. Wenn das angegebene Sicherungsziel seit der letzten Sicherung geändert wurde, müssen Sie einen Sicherungstyp auswählen. Diese Optionen werden nur aktiviert, wenn Sie das Sicherungsziel ändern. Es stehen die Optionen "Vollständige Sicherung" und "Zuwachssicherung" zur Verfügung.

- **Vollständige Sicherung:** Gibt an, dass die nächste Sicherung eine vollständige Sicherung ist. Das neue Sicherungsziel ist vom alten Sicherungsziel unabhängig. Wenn Sie mit einer vollständigen Sicherung fortfahren, wird der frühere Speicherplatz nicht mehr benötigt, um mit den Sicherungen fortzufahren. Je nachdem, ob Sie die alte Sicherung für spätere Sicherungen verwenden möchten, können Sie sie aufbewahren oder löschen. Dies hat keinerlei Auswirkungen auf zukünftige Sicherungen.

- **Zuwachssicherung:** Gibt an, dass die nächste Sicherung eine Zuwachssicherung ist. Die nächste Zuwachssicherung wird auf dem neuen Sicherungsziel durchgeführt, ohne alle Sicherungen vom vorherigen Ziel zu kopieren. Der neue Speicherort ist jedoch vom vorherigen Ziel abhängig, da die Änderungen nur die Zuwachsdaten (und nicht die Daten einer vollständigen Sicherung) beinhalten. Löschen Sie die Daten nicht vom früheren Speicherort. Wenn Sie das Sicherungsziel in einen anderen Ordner verschieben und eine Zuwachssicherung durchführen möchten, das frühere Sicherungsziel aber nicht mehr existiert, so schlägt die Sicherung fehl.

4. Geben Sie die **Sicherungsquelle** an.

   Sie können den gesamten Computer oder einzelne Volumes auf Ihrem Computer für die Sicherung angeben.

   - **Gesamten Rechner sichern:** Mit dieser Option wird der gesamte Rechner gesichert. Alle Volumes des Rechners werden gesichert.

     Hinweis: Wenn die Option zur Sicherung des gesamten Rechners ausgewählt wird, erkennt CA ARCserve D2D automatisch alle Datenträger/Volumes, die an den derzeitigen Rechner angeschlossen sind und nimmt sie in die Sicherung auf.

     Wenn zum Beispiel ein neuer Datenträger an den Rechner angeschlossen wird, nachdem die Sicherungseinstellungen festgelegt wurden, müssen Sie die Einstellungen nicht erneut ändern und die Daten auf dem neuen Datenträger werden automatisch geschützt.

   - **Einzelne Volumes zur Sicherung auswählen:** Mit der Funktion des Volumefilters können Sie einzelne Volumes zur Sicherung auswählen. Wenn Sie ein Volume angeben, das im CA ARCserve D2D-Remote-Server nicht vorhanden ist, springt das Volume jedoch während Sicherung automatisch weiter. Geben Sie zum Beispiel an, die Volumes C, D und E zu sichern; und weisen Sie sie dem CA ARCserve D2D-Server zu, der nur die Volumes C und D enthält. Die Richtlinie wird den Volumes C und D zum CA ARCserve D2D-Server zugewiesen und Volume E wird mit einer Warnmeldung im Aktivitätsprotokoll gespeichert und übersprungen.

     Sie haben auch die Möglichkeit, alle aufgelisteten Volumes auszuwählen oder die Auswahl aller Volumes aufzuheben.

     Hinweis: Wenn bestimmte Volumes speziell für die Sicherung ausgewählt werden, werden auch nur diese angegebenen Volumes gesichert.

     Eine Benachrichtigung wird für die folgende Bedingung angezeigt:

     - **BMR:** Wenn das System-/Startvolume nicht zur Sicherung ausgewählt ist, werden Sie über einen Warnhinweis darauf aufmerksam gemacht, dass die Sicherung nicht für BMR verwendet werden kann.

5. Geben Sie die **Einstellungen für die Aufbewahrung** an.

   Sie können die Aufbewahrungsrichtlinie festlegen, die auf der Anzahl der aufzubewahrenden Wiederherstellungspunkte basiert (führt Sitzungen zusammen), oder die auf der Anzahl der aufzubewahrenden Wiederherstellungssätze basiert (löscht Wiederherstellungssätze und deaktiviert unendliche Zuwachssicherungen).

   - Wiederherstellungspunkt – Dies ist die empfohlene Option. Wenn diese Option ausgewählt ist, können Sie die unendlichen Zuwachssicherungsmöglichkeiten voll ausnutzen und sparen Speicherplatz.
   - Wiederherstellungssatz – Diese Option wird im Allgemeinen für große Speicherumgebungen verwendet. Wenn diese Option ausgewählt ist, können Sie Sicherungssätze erstellen und verwalten, die Ihnen dabei helfen, Ihre Zeit für das Sicherungsfenster effizienter zu verwalten, wenn Sie eine große Datenmenge schützen. Sie können diese Option verwenden, wenn Sicherungszeit eine Priorität über Speicherplatzeinschränkungen ist.

   Standard: Wiederherstellungspunkte aufbewahren

   Wiederherstellungspunkte aufbewahren

   Wählen Sie diese Option aus, um die Anzahl von Wiederherstellungspunkten (vollständig, inkrementell und Überprüfungssicherungs-Images) anzugeben, die aufbewahrt werden sollen.

   - **Geben Sie die Anzahl der Wiederherstellungspunkte an, die aufbewahrt werden sollen**

     Wird die maximale Anzahl überschritten, so fügt CA ARCserve D2D die früheste (älteste) untergeordnete Zuwachssicherung in die übergeordnete Sicherung ein und erstellt ein neues Baseline-Image, das aus den übergeordneten Blöcken und dem ältesten untergeordneten Block besteht. Das Einfügen des ältesten untergeordneten Blocks in die übergeordnete Sicherung ist ein Zyklus, der sich bei allen folgenden Sicherungen wiederholt. Sie können dadurch unendlich viele Zuwachssicherungen durchführen, ohne die Aufbewahrungszeit zu verändern.

     Hinweis: Wenn auf Ihrem Ziel nicht genügend freier Speicherplatz zur Verfügung steht, sollten Sie in Betracht ziehen, die Anzahl der gespeicherten Wiederherstellungspunkte zu reduzieren.

     Standard: 31

     Minimum: 1

     Maximum: 1344

- **Zusammenführungsjob ausführen:** Wählen Sie eine der folgenden Optionen, wenn Sie den Zusammenführungsjob ausführen:
  - **So früh wie möglich:** Wählen Sie diese Option, um den Zusammenführungsjob nun jederzeit auszuführen.
  - **Täglich innerhalb des folgenden Zeitrahmens:** Wählen Sie diese Option, um den Zusammenführungsjob in einem festgelegten Zeitraum auszuführen. Das Festlegen eines Zeitraums vermeidet, dass der Zusammenführungsjob zu viele EA-Operationen in den Produktionsserver einfügt, wenn der Zusammenführungsjob über einen langen Zeitraum hinweg ausgeführt wird.

    Hinweis: Wenn Sie den Zeitbereich festlegen, um den Zusammenführungsjob auszuführen, stellen Sie sicher, dass Sie einen Zeitbereich angeben, der es den zugehörigen Sicherungsjobs ermöglicht, abzuschließen, bevor die Zusammenführung beginnt.

Wiederherstellungssätze aufbewahren

Wählen Sie diese Option, um die Anzahl der aufzubewahrenden Wiederherstellungssätze festzulegen. Mit dieser Einstellung können Sie unendliche Zuwachssicherungen deaktivieren, ohne Sitzungen zusammenzuführen. Die Verwendung von Wiederherstellungssätzen löst die Zeit, die zur Fertigstellung von Zusammenführungsjobs benötigt wird.

- **Geben Sie die Anzahl der Wiederherstellungssätze an, die aufbewahrt werden sollen**

  Wählen Sie diese Option, um die Anzahl der aufbewahrten Wiederherstellungssätze festzulegen. Ein Wiederherstellungssatz ist eine Reihe von Sicherungen: anfangs eine vollständige Sicherung gefolgt von einer Reihe von Zuwachs-, Überprüfungs- oder vollständigen Sicherungen.

  Beispiel-Satz 1:

  - Vollständige Sicherung
  - Zuwachssicherung
  - Zuwachssicherung
  - Überprüfen
  - Zuwachssicherung

Beispiel-Satz 2:

- Vollständige Sicherung
- Zuwachssicherung
- Vollständige Sicherung
- Zuwachssicherung

Eine vollständige Sicherung ist erforderlich, um einen neuen Wiederherstellungssatz zu starten. Die Sicherung, die den Satz startet, wird automatisch in eine vollständige Sicherung konvertiert, auch wenn für diesen Zeitpunkt keine vollständige Sicherung zur Ausführung konfiguriert oder geplant ist.

Hinweis: Ein unvollständiger Wiederherstellungssatz wird nicht mitgezählt, wenn ein vorhandener Wiederherstellungssatz berechnet wird. Ein Wiederherstellungssatz wird nur als vollständig erachtet, wenn die Anfangssicherung des nächsten Wiederherstellungssatzes erstellt wird.

Standardeinstellung: 2

Minimum: 1

Maximum: 100

Hinweis: Wenn Sie einen Wiederherstellungssatz löschen wollen, um Sicherungsspeicherplatz zu sparen, reduzieren Sie die Anzahl von aufbewahrten Sätzen. Somit löscht CA ARCserve D2D automatisch den ältesten Wiederherstellungssatz. Versuchen Sie nicht, den Wiederherstellungssatz manuell zu löschen.

Beispiel 1 - Wiederherstellungssatz:

- Die Startzeit der Sicherung ist 06:00 Uhr, 20. August 2012.
- Eine Zuwachssicherung wird alle 12 Stunden ausgeführt.
- Ein neuer Wiederherstellungssatz beginnt bei der letzten Sicherung am Freitag.
- Sie wollen drei Wiederherstellungssätze aufbewahren.

In diesem Beispiel wird eine Zuwachssicherung jeden Tag um 06:00 Uhr und um 18:00 Uhr ausgeführt. Der erste Wiederherstellungssatz wird erstellt, wenn die erste Sicherung (muss eine vollständige Sicherung sein) durchgeführt wurde. Dann wird die erste vollständige Sicherung als die Anfangssicherung des Wiederherstellungssatzes markiert. Wenn die am Freitag um 18:00 geplante Sicherung ausgeführt wird, wird sie in eine vollständige Sicherung konvertiert und die Sicherung wird als Anfangssicherung des Wiederherstellungssatzes markiert.

Beispiel 2 - Wiederherstellungssatz:

- Legen Sie die Zahl der Wiederherstellungssätze, die aufbewahrt werden sollen, auf 1 fest.

Hinweis: CA ARCserve D2D behält immer zwei Sätze, sodass ein vollständiger Satz behalten wird, bevor der nächste Wiederherstellungssatz gestartet wird.

Beispiel 3 - Wiederherstellungssatz:

- Legen Sie die Zahl der Wiederherstellungssätze, die aufbewahrt werden sollen, auf 2 fest.

Hinweis: CA ARCserve D2D löscht den ersten Wiederherstellungssatz, wenn der vierte Wiederherstellungssatz dabei ist, zu starten. Durch die Ausführung dieser Aktion wird sichergestellt, dass, wenn die erste Sicherung gelöscht und die vierte Sicherung gestartet wird, noch zwei verfügbare Wiederherstellungssätze (Wiederherstellungssatz 2 und Wiederherstellungssatz 3) auf dem Datenträger vorhanden sind.

Auch wenn Sie nur einen Wiederherstellungssatz aufbewahren, benötigen Sie Speicherplatz für mindestens zwei vollständige Sicherungen.

- **Einen neuen Wiederherstellungssatz starten jeden:**:
  - **Ausgewählten Tag der Woche** Legt den Wochentag fest, der ausgewählt ist, um einen neuen Wiederherstellungssatz zu starten.
  - **Ausgewählten Tag des Monats** Legt den Tag des Monats fest, der ausgewählt ist, um einen neuen Wiederherstellungssatz zu starten. Legen Sie 1 bis 30 fest, oder wenn ein Monat 28, 29, 30 oder 31 Tage hat, können Sie den letzten Tag des Monats als den Tag angeben, um den Wiederherstellungssatz zu erstellen.
- **Einen neuen Wiederherstellungssatz starten mit:**
  - **Erste Sicherung am ausgewählten Tag:** Legt den Wochentag fest, der ausgewählt ist, um einen neuen Wiederherstellungssatz zu starten.
  - **Letzte Sicherung am ausgewählten Tag:** Zeigt an, dass Sie einen neuen Wiederherstellungssatz mit der letzten geplanten Sicherung am angegebenen Tag starten wollen. Wenn die letzte Sicherung für das Starten des Satzes ausgewählt ist und die letzte Sicherung aus irgendeinem Grund fehlschlägt, startet die nächste geplante Sicherung den Satz, indem der Satz in eine vollständige Sicherung konvertiert wird. Wenn die nächste Sicherung Ad-Hoc ausgeführt wird (wenn zum Beispiel in einer Notfallsituation eine schnelle Zuwachssicherung erforderlich ist), können Sie bestimmen, ob Sie eine vollständige Sicherung ausführen möchten, um den Wiederherstellungssatz zu starten, oder ob Sie eine Zuwachssicherung ausführen möchten, sodass die nächste Sicherung den Wiederherstellungssatz startet.

Hinweis: Die letzte Sicherung ist möglicherweise nicht die letzte Sicherung des Tages, wenn Sie eine Ad-Hoc-Sicherung ausführen.

6. Geben Sie die Art der **Komprimierung** an.

   Geben Sie den Komprimierungstyp an, den Sie für Sicherungen verwenden möchten.

   Durch eine Komprimierung wird der verwendete Speicherplatz verringert. Dies hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit der Sicherung.

   Es stehen folgende Komprimierungsoptionen zur Verfügung:

   - **Keine Komprimierung**

     Es wird keine Komprimierung durchgeführt. Diese Option bedeutet niedrigste CPU-Auslastung (höchste Geschwindigkeit), aber auch höchste Speicherplatzverwendung für Ihr Sicherungs-Image.

   - **Standard-Komprimierung**

     Es wird eine Komprimierung bis zu einem gewissen Grad ausgeführt. Diese Option bietet ein Gleichgewicht zwischen CPU-Auslastung und verwendetem Speicherplatz. Dies ist die Standardeinstellung.

   - **Maximale Komprimierung**

     Es wird eine maximale Komprimierung durchgeführt. Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigste Speicherplatzverwendung für Ihr Sicherungs-Image.

   Beachten Sie dabei folgendes Szenarien:

   - Wenn Ihr Sicherungs-Image nicht komprimierbare Daten wie z. B. .jpg- oder .zip-Dateien enthält, muss für die Verarbeitung dieser Daten zusätzlicher Speicherplatz zugewiesen werden. Wenn Sie Komprimierungsoptionen angeben und die Sicherungsquelle Daten enthält, die nicht komprimiert werden können, werden Sie eine Gesamtzunahme an Festplattenspeicherauslastung bemerken.
   - Wenn Sie die Komprimierungsebene von "Keiner Komprimierung" auf "Standard-Komprimierung" oder "Maximale Komprimierung" ändern, oder wenn Sie die Komprimierungsebene von "Standard-Komprimierung" oder "Maximale Komprimierung" auf "Keine Komprimierung" ändern, wird die erste Sicherung, die nach der Änderung der Komprimierungsebene durchgeführt wird, eine vollständige Sicherung sein. Nachdem diese vollständige Sicherung durchgeführt wurde, werden alle weiteren Sicherungen (vollständige Sicherung, Zuwachssicherung oder Überprüfungssicherung) gemäß dem Ablaufplan durchgeführt.
   - Wenn auf Ihrem Ziel nicht genügend freier Speicherplatz zur Verfügung steht, sollten Sie in Betracht ziehen, die Einstellung "Komprimierung" der Sicherung zu erhöhen.

7. Geben Sie die Einstellungen zur **Verschlüsselung** an.

   a. Wählen Sie den Verschlüsselungsalgorithmus aus, den Sie für Sicherungen verwenden möchten.

      Bei der Datenverschlüsselung werden Daten in ein Format umgewandelt, das ohne den entsprechenden Entschlüsselungsmechanismus nicht verständlich ist. CA ARCserve D2D-Datenschutz verwendet sichere AES-Verschlüsselungsalgorithmen (AES steht im Englischen für Advanced Encryption Standard), um größtmögliche Sicherheit und Datenschutz für Ihre angegebenen Daten zu erreichen.

      Die verfügbaren Formatoptionen sind "Keine Verschlüsselung", "AES-128", "AES-192" und "AES-256". (Um die Verschlüsselung zu deaktivieren, wählen Sie "Keine Verschlüsselung" aus).

      - Eine vollständige Sicherung und alle verknüpften Zuwachs- und Überprüfungssicherungen müssen den gleichen Verschlüsselungsalgorithmus verwenden.
      - Wenn der Verschlüsselungsalgorithmus für eine Zuwachs- oder Überprüfungssicherung geändert wird, muss eine vollständige Sicherung ausgeführt werden. Dies bedeutet, dass nach einer Änderung des Verschlüsselungsalgorithmus die erste Sicherung trotz des ursprünglichen Sicherungstyps vollständig ist.

        Wenn Sie zum Beispiel das Algorithmusformat ändern und eine angepasste Zuwachs- oder Überprüfungssicherung manuell übergeben, wird automatisch auf eine vollständige Sicherung gewechselt.

   b. Wenn ein Verschlüsselungsalgorithmus ausgewählt wird, müssen Sie ein Verschlüsselungskennwort angeben (und es bestätigen).

      - Das Verschlüsselungskennwort kann höchstens aus 23 Zeichen bestehen.
      - Eine vollständige Sicherung und alle verknüpften Zuwachs- und Überprüfungssicherungen müssen das gleiche Kennwort zur Datenverschlüsselung verwenden.
      - Wenn das Verschlüsselungskennwort für eine Zuwachs- oder Überprüfungssicherung geändert wird, muss eine vollständige Sicherung ausgeführt werden. Dies bedeutet, dass nach einer Änderung des Verschlüsselungskennworts die erste Sicherung trotz des ursprünglichen Sicherungstyps vollständig ist.

        Wenn Sie zum Beispiel das Verschlüsselungskennwort ändern und eine angepasste Zuwachs- oder Überprüfungssicherung manuell übergeben, wird automatisch auf eine vollständige Sicherung gewechselt.

c. CA ARCserve D2D verfügt über Verschlüsselungskennwortverwaltung, damit Sie sich die Verschlüsselungskennwörter nicht zu merken brauchen.

- Das Kennwort wird auch verschlüsselt.
- Das Kennwort wird gespeichert und ist nicht erforderlich, wenn Sie auf dem gleichen Rechner wiederherstellen.
- Das Kennwort wird benötigt, wenn Sie auf einem anderen Rechner wiederherstellen.
- Das Kennwort wird nicht benötigt, wenn Sie versuchen, einen Wiederherstellungspunkt zu exportieren, der verschlüsselte Daten enthält, und der Wiederherstellungspunkt zu Sicherungen gehört, die auf dem aktuellen Rechner ausgeführt wurden.
- Das Kennwort wird immer benötigt, wenn Sie versuchen, verschlüsselte Daten von einem exportierten Wiederherstellungspunkt wiederzuherstellen.
- Das Kennwort ist nicht erforderlich, um zu einem verschlüsselten Wiederherstellungspunkt zu wechseln.
- Das Kennwort ist erforderlich, um eine BMR auszuführen.

d. Wenn die Verschlüsselung aktiviert ist, wird das Aktivitätsprotokoll aktualisiert.

- Eine Meldung wird im Aktivitätsprotokoll aufgezeichnet, um den ausgewählten Verschlüsselungsalgorithmus für jede Sicherung zu beschreiben.
- Eine Meldung wird im Aktivitätsprotokoll aufgezeichnet, um anzugeben, warum eine Zuwachs- oder Überprüfungssicherung in eine vollständige Sicherung umgewandelt wurde (Kennwortänderung oder Algorithmusänderung).

Hinweis: Die Verschlüsselungseinstellungen müssen nicht für alle Ihre Sicherungen gleich bleiben. Sie können diese Einstellungen jederzeit ändern, auch nach einigen Sicherungen der gleichen Daten.

8. Machen Sie Angaben zu **Sicherung drosseln**.

   Sie können die Höchstgeschwindigkeit festlegen (MB/Min), mit der Sicherungen geschrieben werden. Sie können die Sicherungsgeschwindigkeit drosseln, um die CPU- oder Netzwerkauslastung zu reduzieren. Allerdings wirkt sich die Einschränkung der Sicherungsgeschwindigkeit negativ auf das Sicherungsfenster aus. Wenn Sie die maximale Sicherungsgeschwindigkeit herabsetzen, wird die zur Ausführung der Sicherung benötigte Zeit länger.

   Hinweis: Standardmäßig ist die Option "Sicherung drosseln" nicht aktiviert und die Sicherungsgeschwindigkeit wird nicht gesteuert.

9. Klicken Sie auf "Speichern".

Die Schutzeinstellungen wurden gespeichert.

Festlegen von Sicherungsablaufplänen

Mit CA ARCserve Central Protection Manager können Sie Ablaufpläne für Ihre Sicherungen festlegen.

So legen Sie Sicherungsablaufpläne fest

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

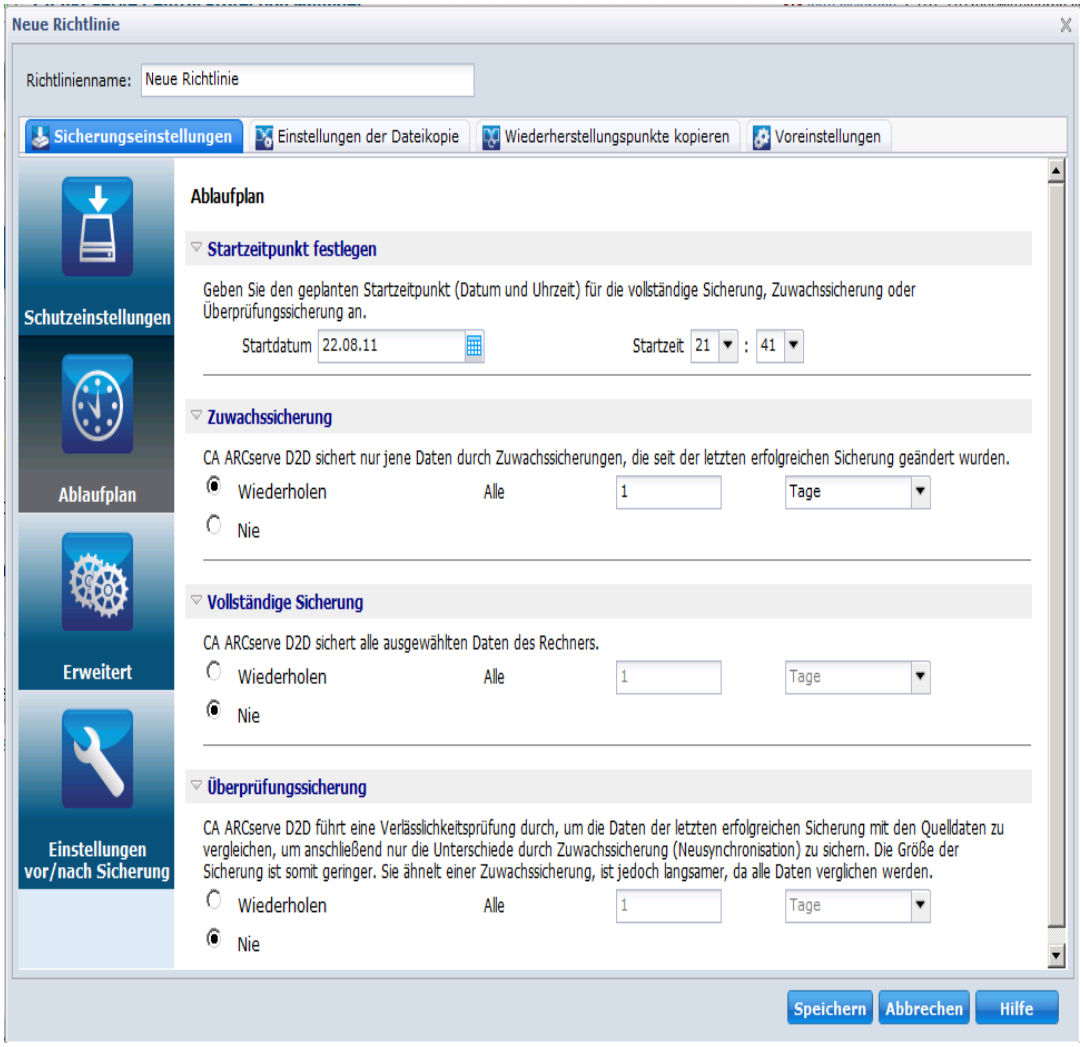
   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Klicken Sie auf die Registerkarte "Ablaufplan".

   Das Optionsdialogfeld "Ablaufplan" wird geöffnet.



4. Legen Sie Ihre Ablaufplanoptionen fest:

   - **Startzeitpunkt festlegen:** Legt das Startdatum und die Startzeit für Ihre geplanten Sicherungen fest.

     Hinweis: Beim Festlegen des Intervalls zwischen wiederholten Sicherungsjobs sollten Sie sicherstellen, dass Sie genug Zeit einkalkulieren, damit der vorherige Job und alle zugehörigen Zusammenführungsjobs abschließen können, bevor der nächste Sicherungsjob startet. Sie können diesen Zeitraum auf der Basis Ihrer eigenen spezifischen Sicherungsumgebung und dem Verlauf berechnen.

   - **Zuwachssicherung:** Legt den Sicherungsablaufplan für Zuwachssicherungen fest.

     Als Teil eines Ablaufplans erstellt CA ARCserve D2D nur Zuwachssicherungen von jenen Blöcken, die seit der letzten erfolgreichen Sicherung geändert wurden. Die Vorteile von Zuwachssicherungen bestehen darin, dass sie sehr schnell durchgeführt werden und ein sehr kleines Sicherungs-Image erstellen. Es ist die optimale Methode zur Durchführung von Sicherungen, die standardmäßig verwendet werden sollte.

     Es stehen die Optionen "Wiederholen" und "Nie" zur Verfügung. Wenn Sie "Wiederholen" auswählen, müssen Sie auch die Zeitspanne (Minuten, Stunden oder Tage) zwischen den Sicherungsversuchen festlegen. Das Mindestintervall für Zuwachssicherungen ist 15 Minuten.

     Standardmäßig sind tägliche Zuwachssicherungen geplant.

   - **Vollständige Sicherung:** Legt den Sicherungsablaufplan für vollständige Sicherungen fest.

     CA ARCserve D2D führt wie geplant eine vollständige Sicherung aller verwendeten Blöcke des Quellrechners durch. Es stehen die Optionen "Wiederholen" und "Nie" zur Verfügung. Wenn Sie "Wiederholen" auswählen, müssen Sie auch die Zeitspanne (Minuten, Stunden oder Tage) zwischen den Sicherungsversuchen festlegen. Das Mindestintervall für vollständige Sicherungen ist 15 Minuten.

     Standardmäßig ist der Ablaufplan für vollständige Sicherungen "Nie" (keine Wiederholung geplant).

   - **Überprüfungssicherung**: Legt den Sicherungsablaufplan für Überprüfungssicherungen fest.

Als Teil eines Ablaufplans wird CA ARCserve D2D die Gültigkeit und Vollständigkeit der geschützten Daten durch einen Vergleich des gespeicherten Sicherungs-Images mit der Sicherungsquelle überprüfen und das Image, wenn erforderlich, neu synchronisieren. Bei einer Überprüfungssicherung wird die letzte Sicherung jedes einzelnen Blocks mit den Inhalten und Informationen der Quelle verglichen. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht (wahrscheinlich aufgrund von Änderungen seit der letzten Sicherung), aktualisiert CA ARCserve D2D die Sicherung dieses Blocks (Neusynchronisierung). In sehr seltenen Fällen kann eine Überprüfungssicherung auch durchgeführt werden, um eine vollständige Sicherung zu erhalten, ohne den entsprechenden Speicherplatz zu verwenden.

Der Vorteil von Überprüfungssicherungen besteht darin, dass im Vergleich zu vollständigen Sicherungen ein sehr kleines Sicherungs-Image erstellt wird, da nur die geänderten Blöcke (d. h., jene Blöcke, die nicht mit der letzten vollständigen Sicherung übereinstimmen) gesichert werden. Der Nachteil einer Überprüfungssicherung besteht darin, dass sie viel Zeit benötigt, da CA ARCserve D2D alle Blöcke des Quelldatenträgers mit den Blöcken der letzten Sicherung vergleichen muss.

Es stehen die Optionen "Wiederholen" und "Nie" zur Verfügung. Wenn Sie "Wiederholen" auswählen, müssen Sie auch die Zeitspanne (Minuten, Stunden oder Tage) zwischen den Sicherungsversuchen festlegen. Das Mindestintervall für Überprüfungssicherungen ist 15 Minuten.

Standardmäßig ist der Ablaufplan für Überprüfungssicherungen "Nie" (keine Wiederholung geplant).

5. Klicken Sie auf "Speichern".

Die Einstellungen für den Sicherungsablaufplan wurden gespeichert.

Hinweis: Wenn für denselben Zeitpunkt mehrere Sicherungstypen geplant sind, gelten die folgenden Prioritäten:

- Priorität 1 - Vollständige Sicherung
- Priorität 2 - Überprüfungssicherung
- Priorität 3 - Zuwachssicherung

Wenn z. B. alle drei Sicherungstypen für denselben Zeitpunkt geplant sind, führt CA ARCserve D2D eine vollständige Sicherung durch. Wenn keine vollständige Sicherung, aber eine Überprüfungssicherung und eine Zuwachssicherung geplant sind, führt CA ARCserve D2D die Überprüfungssicherung durch. Eine geplante Zuwachssicherung wird nur dann durchgeführt, wenn keine Konflikte mit anderen Sicherungstypen bestehen.

Festlegen der erweiterten Sicherungseinstellungen

Mit CA ARCserve Central Protection Manager können Sie erweiterte Einstellungen für Ihre Sicherungen festlegen.

So legen Sie erweiterte Sicherungseinstellungen fest

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

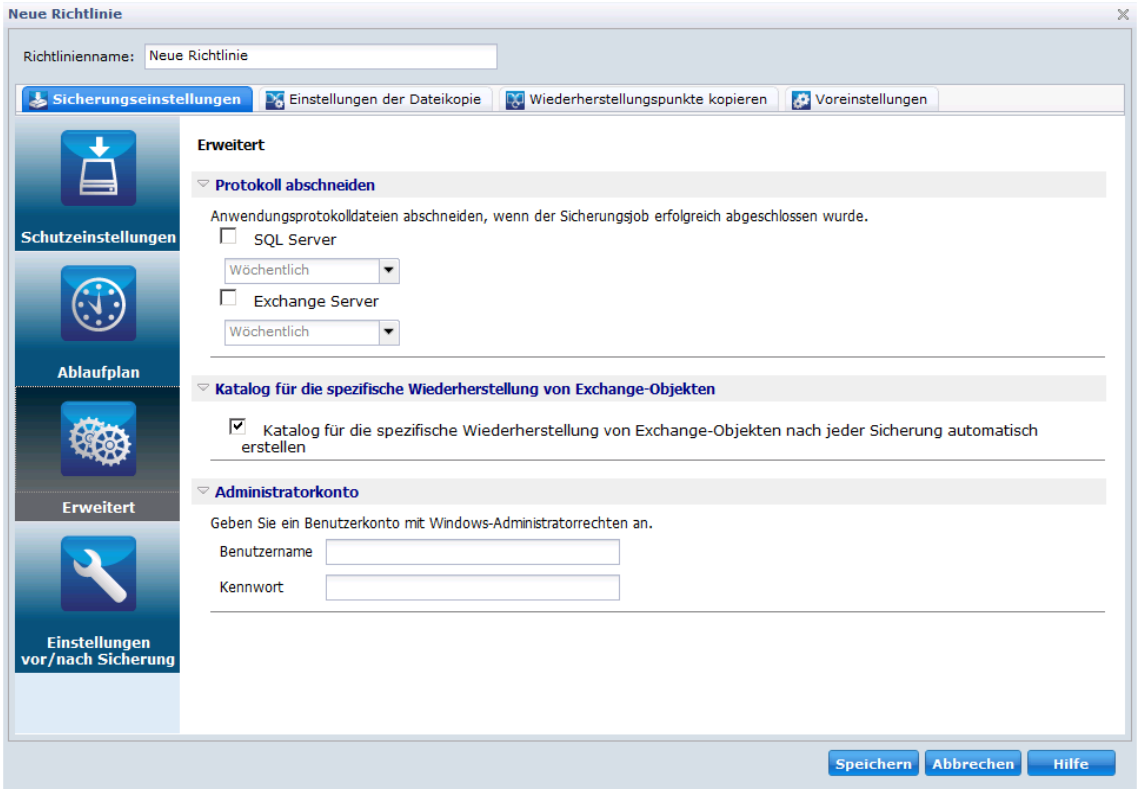
   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Klicken Sie auf die Registerkarte "Erweitert".

   Das Dialogfeld "Erweiterte Einstellungen" wird geöffnet.



4. Geben Sie die erweiterten Aktionseinstellungsoptionen an.

   - **Protokoll abschneiden:** Mit dieser Option können Sie festlegen, dass das die akkumulierten Transaktionsprotokolldateien für die ausgewählten Anwendungen nach der nächsten erfolgreichen Sicherung abgeschnitten werden.

     CA ARCserve D2D-Sicherungen bestehen aus einem Snapshot-Image und den Transaktionsprotokolldateien, die dafür erstellt wurden. Ab einem gewissen Zeitpunkt werden die älteren (übergebenen) Transaktionsprotokolldateien nicht mehr benötigt und können gelöscht werden, um Platz für neue Protokolldateien zu schaffen. Das Löschen dieser Protokolldateien wird als "Abschneiden" bezeichnet. Diese Option aktiviert das Abschneiden übergebener Transaktionsprotokolldateien, um Speicherplatz frei zu machen.

     Es stehen die Optionen "SQL Server" und "Exchange Server" zur Verfügung. Sie können eine, beide oder keine dieser Optionen auswählen. Wenn Sie eine dieser Optionen auswählen, können Sie einen Zeitintervall (täglich, wöchentlich oder monatlich) für das automatische Abschneiden von Protokollen planen:

     Hinweis: Damit die Transaktionsprotokolldateien abgeschnitten werden können, muss eine erfolgreiche Sicherung durchgeführt werden.

     - **Täglich** - Jeden Tag nachdem eine Sicherung erfolgreich abgeschlossen wurde, werden die übergebenen Transaktionsprotokolle sofort gelöscht.
     - **Wöchentlich** - 7 Tage nachdem die Sicherung erfolgreich abgeschlossen wurde, werden die übergebenen Transaktionsprotokolle sofort gelöscht.
     - **Wöchentlich** - 30 Tage nachdem die Sicherung erfolgreich abgeschlossen wurde, werden die übergebenen Transaktionsprotokolle sofort gelöscht.

     Wenn zum Zeitpunkt der geplanten Löschung bereits ein Sicherungsjob ausgeführt wird, wird der Löschvorgang auf den nächsten geplanten Job verschoben.

     Beispiel:

     Wenn Sie eine Zuwachssicherung geplant haben, die täglich um 17 Uhr automatisch ausgeführt werden soll und eine vollständige Sicherung um 16:55 Uhr manuell gestartet wird, können Sie davon ausgehen, dass die Sicherung um 17:10 Uhr erfolgreich abgeschlossen wird.

     In diesem Fall wird die Zuwachssicherung, die für 17 Uhr geplant war, nicht ausgeführt, da die vollständige Ad-Hoc-Sicherung noch ausgeführt wird. Die übergebenen Transaktionsprotokolle werden nach dem nächsten erfolgreichen Sicherungsjobs gelöscht. In diesem Fall geschieht dies am nächsten Tag, nachdem die geplante Zuwachssicherung um 17 Uhr erfolgreich abgeschlossen wurde.

- **Spezifische Wiederherstellung von Exchange-Objekten:** Gibt an, ob Sicherungen der spezifischen Wiederherstellung von Exchange-Objekten aktiviert werden sollen (generiert die Kataloge für die spezifische Wiederherstellung von Exchange).

  Eine Sicherung spezifischer Wiederherstellungen von Exchange-Objekten erfasst Informationen zur E-Mail-Meldung, zum E-Mail-Ordner und zu den Postfachebenen von Exchange in einer einzelnen Sicherung über die Exchange-Datenbank. Wenn diese Option aktiviert ist, können Sie detaillierte Wiederherstellungen der Exchange-Datenbank durchführen, indem Sie in einer Liste von Objekten in Exchange auswählen und angeben, was Sie wiederherstellen möchten, ohne zuerst die Exchange-Datenbank an einem alternativen Speicherort wiederherstellen oder einen Speicherauszug erstellen zu müssen.

  - Der Vorteil der Aktivierung dieser Option ist, dass das Durchsuchen von Wiederherstellungen mit einem Katalog für die spezifische Wiederherstellung von Exchange-Objekten nicht lange dauert.
  - Der Nachteil liegt darin, dass das Erstellen von Katalogen für die spezifische Wiederherstellung von Exchange-Objekten für jede Sicherung ein ausgedehntes Sicherungsfenster und eine erhöhte Auslastung bedeutet. CA ARCserve D2D muss jedes Postfach authentifizieren und die detaillierten Informationen aufbauen. Im Angesicht der Anzahl von Postfächern und der Größe von Daten kann dies eine zeitintensive Aufgabe darstellen.
  - Wenn Sie die Option "Spezifische Wiederherstellung von Exchange-Objekten" deaktivieren, werden in CA ARCserve D2D die grundlegenden Informationen für Exchange gespeichert. Bevor Sie eine Wiederherstellung durchführen, haben Sie die Gelegenheit, einen Katalog für die spezifische Wiederherstellung von Exchange-Objekten zu generieren.

- **Administratorkonto:** Legt Benutzername und Kennwort mit Zugriffsrechten zur Durchführung von Sicherungen fest. CA ARCserve D2D stellt sicher, dass Benutzername und Kennwort gültig sind und der Benutzer Mitglied einer Administratorgruppe ist.

  Beachten Sie Folgendes:

  - Um ein Domänenkonto anzugeben, sollten Sie einen vollständigen Domänenbenutzernamen im Format "<Domänenname>\<Benutzername>" für den Benutzernamen angeben.
  - Wenn die Informationen für das Administratorkonto des CA ARCserve D2D-Servers geändert werden (Benutzername/Kennwort), ist es empfehlenswert, auch die Informationen für das Administratorkonto in diesem Dialogfeld neu zu konfigurieren.
  - Wenn Sie die Anmeldeinformationen des Administratorkontos nicht angeben, gibt CA ARCserve D2D automatisch die Informationen des Kontos ein, auf dem die Richtlinie bereitgestellt ist.

5. Klicken Sie auf "Speichern".

Die erweiterten Sicherungseinstellungen wurden gespeichert.

Festlegen von Einstellungen vor/nach der Sicherung

Mit CA ARCserve Central Protection Manager können Sie die Einstellungen für Ihre Sicherungen festlegen.

So legen Sie Einstellungen vor/nach Sicherung fest

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Klicken Sie auf die Registerkarte "Einstellungen vor/nach der Sicherung".

   Das Optionsdialogfeld "Einstellungen vor/nach Sicherung" wird geöffnet.

4. Legen Sie Ihre Sicherungseinstellungen fest.

   - **Aktionen:** Legt Skript-Befehle für Aktionen fest, die vor Beginn der Sicherung, nach Erfassen des Snapshot-Images und/oder nach Abschluss der Sicherung durchgeführt werden sollen. Sie können den Skript-Befehl auch auf der Basis von spezifischen Beendigungscodes auslösen und festlegen, welche Aktion durchgeführt werden soll ("Job ausführen" oder "Job abbrechen"), wenn dieser Beendigungscode zurückgegeben wird.

     - Die Aktion "Job ausführen" weist CA ARCserve D2D an, mit der Ausführung des Jobs fortzufahren, wenn der festgelegte Beendigungscode zurückgegeben wird.

     - Die Aktion "Job abbrechen" weist CA ARCserve D2D an, den Job abzubrechen, wenn der festgelegte Beendigungscode zurückgegeben wird.

5. Klicken Sie auf "Speichern".

Die Einstellungen vor/nach Sicherung wurden gespeichert.

Verwalten der Einstellungen der Dateikopie

Bevor Sie Ihren ersten Dateikopierjob ausführen, müssen Sie die Dateikopiereinstellungen und -richtlinien festlegen. Diese Konfigurationen ermöglichen es Ihnen, Verhaltensfaktoren wie die Quelle Ihrer Dateikopiedaten, das Ziel Ihrer kopierten Dateien, den Ablaufplan für jeden Dateikopierjob, und die Einstellungen und Filter, die auf Ihre Dateikopierjobs angewendet werden, festzulegen. Diese Einstellungen können jederzeit vom Bildschirm "Richtlinien" aus geändert werden.

Festlegen der Quellen der Dateikopie

CA ARCserve Central Protection Manager lässt Sie Quelldateien zur ihrer Dateikopie auf ein bestimmtes Ziel festlegen.

So legen Sie Quellen der Dateikopie fest

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Wählen Sie die Registerkarte "Quelle" der Einstellungen der Dateikopie aus.

   Das Dialogfeld "Quelle" der Einstellungen der Dateikopie öffnet sich.

4. Wählen Sie die Option "Dateikopie aktivieren" aus, um Änderungen an den Einstellungen der Dateikopie zu validieren und zu speichern. Diese Option ist standardmäßig deaktiviert.

5. Legen Sie die Einstellungen für Ihre Dateikopiequelle fest.

   Dateikopienquellen

   Lässt Sie manuell die Dateikopiequellen zusammen mit den entsprechenden Richtlinien (Filter) und dem Typ der Dateikopie (kopieren und beibehalten oder kopieren und verschieben) festlegen, die nach jeder erfolgreich abgeschlossenen CA ARCserve D2D-Sicherung auszuführen ist. Diese Dateikopienquellen können hinzugefügt, entfernt oder geändert werden.

   Hinweis: CA ARCserve D2D kopiert keine Anwendungsdateien, Dateien mit Systemattributen und Dateien mit temporären Attributen.

   - **Quelle hinzufügen**

     Durch Mausklick öffnet sich das Dialogfeld "Richtlinientyp", in dem Sie zuerst den Typ des Dateikopierjobs auswählen können (kopieren und beibehalten oder kopieren und verschieben), der ausgeführt werden soll. Nachdem Sie den Richtlinientyp ausgewählt haben, öffnet sich das entsprechende Dialogfeld "Richtlinie für die Dateikopie", damit Sie eine zu kopierende Quelle hinzufügen und die entsprechenden Richtlinien für diese Quelle festlegen können. Weitere Informationen finden Sie unter Festlegen der Dateikopierichtlinien (siehe Seite 107).

Hinweis: Nur eine aktuell gesicherte Quelle ist zur Dateikopie geeignet. Sie können keine Quelle eines Volumes hinzufügen, das nicht zuvor von CA ARCserve D2D gesichert wurde.

- **Entfernen**

  Durch Mausklick wird die ausgewählte Quelle von der angezeigten Liste entfernt.

- **Ändern**

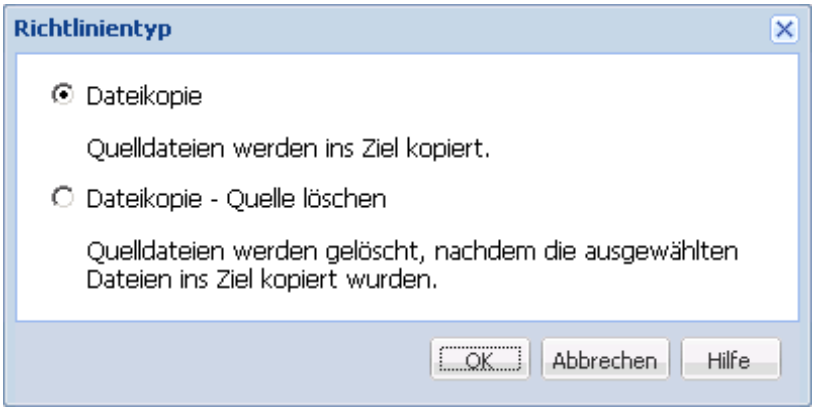
  Durch Mausklick öffnet sich das Dialogfeld "Dateikopierichtlinien", damit Sie die Richtlinieneinstellungen für die ausgewählte Quelle ändern können. Weitere Informationen finden Sie unter Festlegen der Dateikopierichtlinien (siehe Seite 107).

6. Klicken Sie auf "Einstellungen speichern".

Die Einstellungen für die Dateikopie wurden gespeichert.

Festlegen der Dateikopierichtlinien

Wenn Sie für die Dateikopie auf die Option "Quelle hinzufügen" klicken, öffnet sich das Dialogfeld "Richtlinientyp", damit Sie den Typ des auszuführenden Dateikopierjobs auswählen können.



Die verfügbaren Typen sind "Dateikopie" und "Dateikopie - Quelle löschen".

Dateikopie

Daten werden von der Quelle zum Ziel kopiert (bleiben auf Quellspeicherort) und es entstehen mehrere gespeicherte Versionen.

Dateikopie - Quelle löschen

Daten werden von der Quelle zum Ziel verschoben (vom Quellspeicherort gelöscht) und schaffen somit Speicherplatz auf Ihrer Quelle.

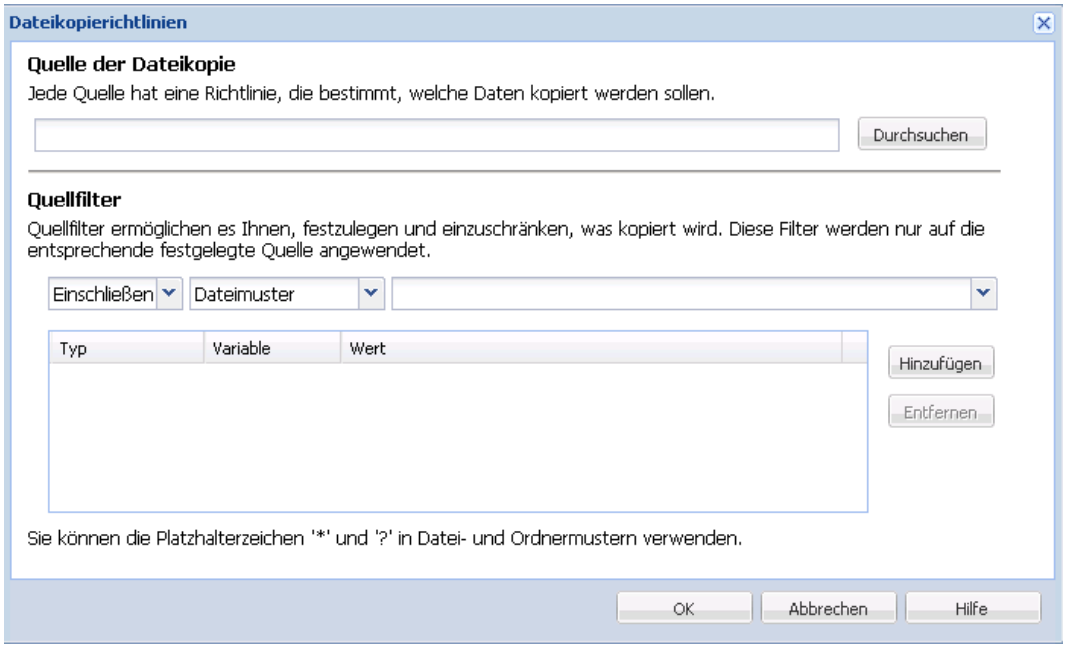
Wenn Sie "Dateikopie - Quelle löschen" auswählen, wird unmittelbar eine Warnmeldung angezeigt, die Sie davor warnt, dass Ihre angegebenen dateikopierten Daten gelöscht werden und am ursprünglichen Quellspeicherort nicht mehr verfügbar sein werden. Sie müssen auf "OK" klicken, um zum Dialogfeld "Dateikopierichtlinien" zu gelangen.

Wichtig! Für Dateien, die mithilfe der Option "Dateikopie - Quelle löschen" kopiert wurden, hinterlässt CA ARCserve D2D eine Stub-Datei mit der Erweiterung "D2DARC". Die Stub-Datei enthält Informationen über das Ziel und darüber, wann die Dateien verschoben wurden.

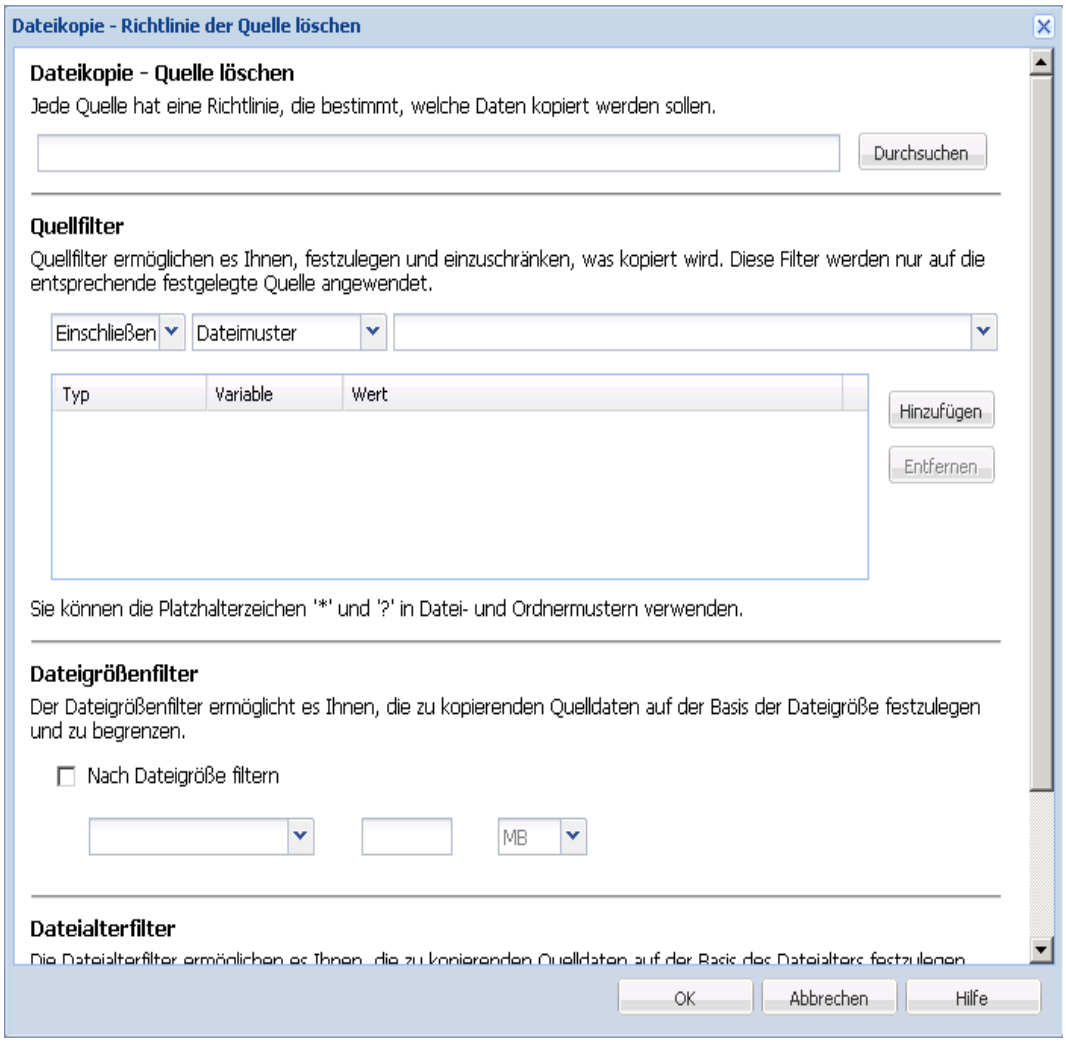
Wenn Sie den Richtlinientyp angeben, um die Quelle Ihrer gesicherten Daten zu löschen, finden Sie dazugehörige Richtlinien, die auch festgelegt werden müssen. Vom Dialogfeld "Einstellungen der Dateikopie" aus können Sie im Dialogfeld "Dateikopierichtlinien", wenn Sie eine neue Dateikopiequelle hinzufügen oder eine vorhandene Dateikopiequelle ändern wollen, die Richtlinien angeben.

Abhängig vom ausgewählten Richtlinientyp öffnet sich ein unterschiedliches Dialogfeld Dateikopierichtlinien"; die Auswahl ist allerdings sehr ähnlich.

"Dateikopie" ausgewählt:



"Dateikopie - Quelle löschen" ausgewählt:

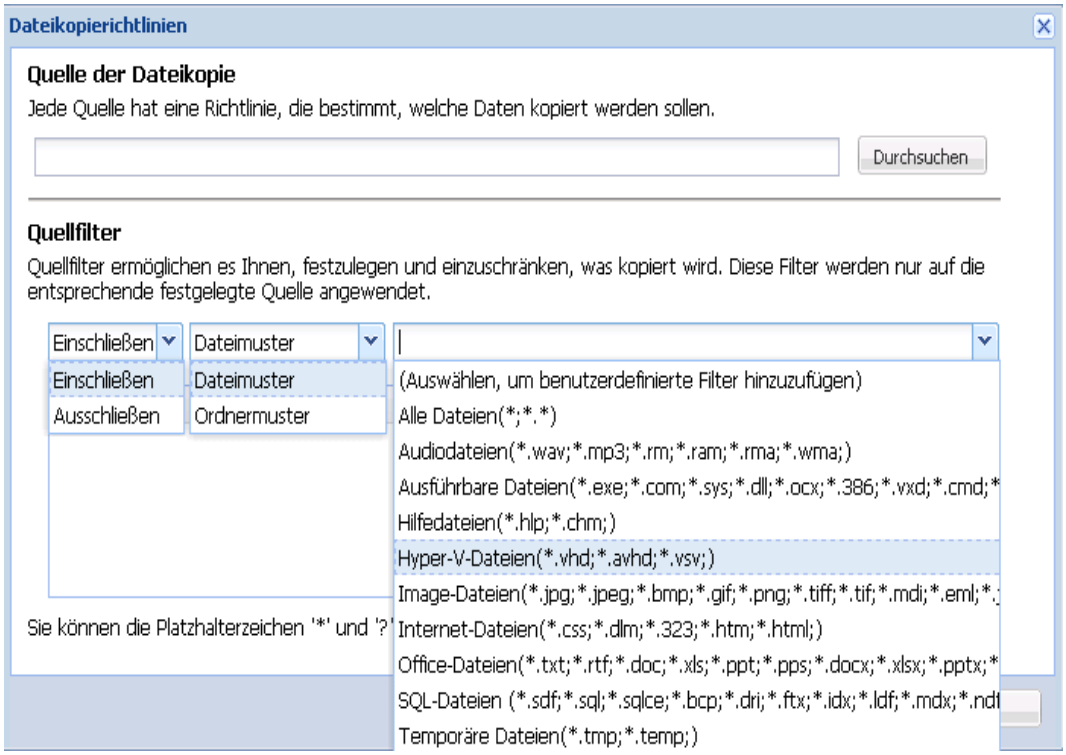

Dateikopie - Richtlinie der Quelle löschen
Dateikopie - Quelle löschen
Jede Quelle hat eine Richtlinie, die bestimmt, welche Daten kopiert werden sollen.
Durchsuchen
Quellfilter
Quellfilter ermöglichen es Ihnen, festzulegen und einzuschränken, was kopiert wird. Diese Filter werden nur auf die entsprechende festgelegte Quelle angewendet.
Einschließen
Dateimuster
Typ
Variable
Wert
Hinzufügen
Entfernen
Sie können die Platzhalterzeichen '*' und '?' in Datei- und Ordnermustern verwenden.
Dateigrößenfilter
Der Dateigrößenfilter ermöglicht es Ihnen, die zu kopierenden Quelldaten auf der Basis der Dateigröße festzulegen und zu begrenzen.
Nach Dateigröße filtern
MB
Dateialterfilter
OK
Abbrechen
Hilfe

Dateikopie - Quelle löschen

Ermöglicht es Ihnen, die Dateikopiequelle festzulegen, sowie die entsprechenden auszuführenden Richtlinien und den Typ der Dateikopie. Sie können nach dem Quellspeicherort durchsuchen.

Quellfilter

Mit Filtern können Sie die zu kopierenden Objekte anhand bestimmter festgelegter Typen und Werte einschränken.



Filtertyp

Es gibt zwei Typen von Filtern: Einschließ- und Ausschlussfilter

Ein Einschließfilter kopiert nur diejenigen Objekte der Dateikopiequelle, die mit den angegebenen Werten übereinstimmen.

Ein Ausschlussfilter kopiert alle Objekte der Dateikopiequelle, außer denen, die mit den angegebenen Werten übereinstimmen.

Sie können innerhalb einer Dateikopieanforderung mehrere Filter festlegen, indem Sie jeden Filterwert mit einem Komma abtrennen.

- Wenn Sie mehrere Einschließfilter festlegen, werden die Daten in die Dateikopie aufgenommen, wenn einer dieser Einschließfilter eine Übereinstimmung erzeugt.
- Wenn Sie mehrere Ausschlussfilter festlegen, werden die Daten von der Dateikopie ausgeschlossen, wenn einer dieser Ausschlussfilter eine Übereinstimmung erzeugt.
- Sie können Einschließfilter und Ausschlussfilter in einer Dateikopieanforderung auch zusammen verwenden.

Hinweis: Wenn die angegebenen Parameter von Einschließfilter und Ausschlussfilter im Konflikt stehen, stellt der Ausschlussfilter immer die höhere Priorität dar und wird durchgesetzt. Ein Einschließfilter kann niemals ein Objekt kopieren, das auch ausgeschlossen wurde.

Filtervariable (Muster)

Es gibt zwei Typen von veränderlichen Musterfiltern: Dateimuster und Ordnermuster

Sie können einen Dateimusterfilter oder Ordnermusterfilter verwenden, um bestimmte Objekte in die Dateikopie einzuschließen oder davon auszuschließen.

Filterwert

Der Filterwert lässt Sie die Informationen eingrenzen, die kopiert werden, dadurch dass nur die Parameterinformationen ausgewählt werden, die Sie festlegen, wie beispielsweise .txt-Dateien.

CA ARCserve D2D unterstützt die Verwendung von Platzhalterzeichen, die dabei helfen, mehrere Objekte auszuwählen, die mit einer einzelnen Anfrage kopiert werden. Ein Platzhalterzeichen ist ein Sonderzeichen, das als Ersatz benutzt werden kann, um entweder ein alleinstehendes Zeichen oder eine Zeichenfolge eines Textes darzustellen.

Die Platzhalterzeichen Sternchen (*) und Fragezeichen (?) werden im Wertefeld unterstützt. Wenn Ihnen der vollständige Datei- oder Ordnermustername nicht bekannt ist, können Sie die Ergebnisse des Filters vereinfachen, indem Sie ein Platzhalterzeichen angeben.

- "*": Verwenden Sie das Sternchen, um null oder mehr Zeichen in dem Wert zu ersetzen.
- "?": Verwenden Sie das Fragezeichen, um ein einzelnes Zeichen in dem Wert zu ersetzen.

Sie können beispielsweise "*.txt" eingeben, um alle Dateien auszuschließen, die eine ".txt" -Erweiterung haben, falls Sie den genauen Dateinamen nicht kennen. Sie können so viele Zeichen des Dateinamens angeben, wie Sie kennen, und die Platzhalter verwenden, um Leerstellen auszufüllen.

Hinweis: Wenn Sie "Dateimuster" als Filtertyp auswählen, ist eine Drop-down-Liste mit vordefinierten Filtern für viele üblicherweise verwendete Dateien verfügbar (MS Office-Dateien, Image-Dateien, ausführbare Dateien, temporäre Dateien etc.).

Dateigrößenfilter (Nur die Jobs "Dateikopie - Quelle löschen")

Dieser Filter bezieht sich nur auf die Jobs "Dateikopie - Quelle löschen" (nicht auf Dateikopierjobs).

Dateigrößenfilter ermöglichen es Ihnen, die zu kopierenden Quellenobjekte auf der Basis der Dateigröße einzuschränken. Wenn Sie den Dateigrößenfilter aktivieren, werden die von Ihnen angegebenen Parameter zu dem Filter, von dem abhängt, welche Objekte in die Dateikopie eingeschlossen werden und welche nicht. Sie können den Bereich auswählen ("Gleich" oder "Größer als", "Gleich" oder "Kleiner als" oder "Zwischen") und dann einen Wert für die Größe eingeben.

Wenn Sie beispielsweise "Gleich oder größer als 10 MB" angeben, kopiert CA ARCserve D2D nur Objekte, die diesen Kriterien entsprechen. Alle anderen Objekte, die diesen Dateigrößenkriterien nicht entsprechen, werden nicht kopiert.

Dateialterfilter (Nur die Jobs "Dateikopie - Quelle löschen")

Dieser Filter bezieht sich nur auf die Jobs "Dateikopie - Quelle löschen" (nicht auf Dateikopierjobs).

Dateialterfilter ermöglichen es Ihnen, zu kopierende Quellobjekte auf der Basis bestimmter Daten der Datei automatisch einzuschließen. Sie können einen Parameter auswählen ("Kein Zugriff auf Dateien in", "Dateien nicht geändert in", und/oder "Dateien nicht erstellt in") und dann einen Wert für die Anzahl an Tagen, Monaten oder Jahren für den Dateialterfilter eingeben. Sie können mehrere Dateialterfilter für automatische Dateikopie auswählen.

Wenn Sie beispielsweise "Dateien nicht geändert in 180 Tagen" angeben, wird CA ARCserve D2D automatisch alle diejenigen Dateien kopieren, die diesen Kriterien entsprechen, d. h. die während der letzten 180 Tage nicht geändert worden sind.

Wichtig! Wenn Sie sowohl Dateigrößen- als auch Dateialterfilter festlegen (oder mehrere Dateialterfilter), werden nur die Dateien kopiert, die allen angegebenen Filterparametern entsprechen. Dateien, die keinem dieser angegebenen Parameter entsprechen, werden nicht kopiert.

Festlegen der Dateikopieziele

Mit CA ARCserve Central Protection Manager können Sie die Zieleinstellungen für die Informationen angeben, die kopiert werden sollen.

So legen Sie Dateikopieziele fest

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Wählen Sie die Registerkarte "Einstellungen der Dateikopie" und danach "Ziel" aus, um das Dialogfeld "Ziel" der Einstellungen der Dateikopie zu öffnen.

4. Geben Sie Ihre Zieleinstellungen an.

   - **Ziel:** Gibt den Zielspeicherort für den Dateikopierjob an. Es kann nur ein Ziel ausgewählt werden.

     Mit CA ARCserve D2D können Sie die Einstellungen der Dateikopie Ihrer gesicherten Dateien auf einen Datenträger oder in die Cloud festlegen. Zur Dateikopie können Sie für Ihre gesicherten Daten "kopieren und beibehalten" oder "kopieren und verschieben" festlegen. Die zwei Prozesse sind ähnlich, mit der Ausnahme, dass die Daten, wenn Sie "kopieren und verschieben" durchführen, von der Quelle zum Ziel verschoben werden (aus dem Quellspeicherort gelöscht werden) und verfügbarer Speicherplatz an Ihrer Quelle entsteht. Wenn Sie "kopieren und beibehalten" auswählen, werden die Daten von der Quelle zum Ziel kopiert (bleiben auf dem Quellenziel erhalten) und es liegen somit mehrere gespeicherte Versionen vor.

     - **Dateikopie auf ein lokales Laufwerk oder Netzwerklaufwerk:** Wenn diese Option ausgewählt ist, können Sie den vollständigen Pfad des Speicherorts angeben, auf den Sie Ihre Quelldateien/-ordner kopieren oder verschieben wollen. Sie können nach diesem Zielspeicherort durchsuchen. Durch Mausklick auf das grüne Pfeilsymbol können Sie die Verbindung zum angegebenen Ziel validieren.

     - **Dateikopie auf Cloud:** Wenn diese Option ausgewählt ist, können Sie den Cloud-Speicherort angeben, auf den Sie Ihre Quelldateien/-ordner kopieren oder verschieben möchten. CA ARCserve D2D unterstützt derzeit Dateikopien zu mehreren Cloud-Anbietern, wie Amazon S3 (Simple Storage Service), Windows Azure, Fujitsu Cloud (Windows Azure) und Eucalyptus-Walrus. Diese Cloud-Anbieter sind öffentlich verfügbare Webservices, mit denen Sie eine beliebige Menge von Daten sicher speichern und diese Daten jederzeit von überall im Netz abrufen können.

       Klicken Sie auf die Schaltfläche "Konfigurieren", um das Dialogfeld "Cloud-Konfiguration" anzuzeigen. Weitere Informationen finden Sie unter Festlegen von Cloud-Konfigurationsdetails für Dateikopie (siehe Seite 116).

       Hinweis: Um einen potenziellen Uhrabweichungsfehler zu beheben, wenn Sie versuchen, eine Verbindung zur Cloud herzustellen, sollten Sie sicherstellen, dass bei Ihrem Rechner die richtige Zeitzone eingestellt ist und die Uhr synchron zur globalen Zeit ist. Sie sollten immer die Zeit Ihres Rechners mit der GMT-Zeit abgleichen. Wenn die Zeit Ihres Rechners nicht mit der korrekten globalen Uhrzeit (auf 5 bis 10 Minuten) synchronisiert ist, funktioniert Amazon S3 nicht. Setzen Sie bei Bedarf die richtige Zeit für Ihren Rechner zurück und wiederholen Sie Ihren Archivierungsjob.

     Falls die Verbindung zum angegebenen Ziel verloren ging oder unterbrochen wurde, versucht CA ARCserve D2D für jede Zieloption einige Male, mit dem Dateikopierjob fortzufahren. Falls diese Neuversuche nicht erfolgreich sind, wird ein Ergänzungsjob von dem Punkt aus ausgeführt werden, an dem der Fehler auftrat. Zusätzlich wird das Aktivitätsprotokoll mit einer entsprechenden Fehlermeldung aktualisiert und es wird eine E-Mail-Benachrichtigung gesendet (falls konfiguriert).

- **Komprimierung:** Legt den Komprimierungstyp für die Dateikopierjobs fest.

  Eine Komprimierung wird normalerweise durchgeführt, um den verwendeten Speicherplatz zu verringern, hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit der Dateikopiejobs.

  Es sind folgende Optionen verfügbar:

  - **Keine Komprimierung**: Es wird keine Komprimierung durchgeführt. Diese Option bedeutet niedrigste CPU-Auslastung (höchste Geschwindigkeit), aber auch höchsten Speicherplatzbedarf für Ihre Dateikopie.
  - **Standard-Komprimierung**: Komprimierung wird bis zu einem gewissen Grad durchgeführt. Diese Option bietet ein Gleichgewicht zwischen CPU-Auslastung und erforderlichem Speicherplatz. Dies ist die Standardeinstellung.
  - **Maximale Komprimierung**: Es wird eine maximale Komprimierung durchgeführt. Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigsten Speicherplatzbedarf für Ihre Dateikopie.

- **Verschlüsselung:** Ermöglicht es Ihnen, Ihr Verschlüsselungskennwort für die Dateikopie zu aktivieren.

- **Aufbewahrungszeit**: Diese Einstellung bezieht sich nur auf kopierte Daten, die verschoben werden (nicht auf Daten, die aufbewahrt werden).

  Gibt die Länge der Zeit (Jahre, Monate, Wochen, Tage) an, während der die gespeicherten Daten am Zielspeicherort aufbewahrt werden. Nach Ablauf der angegebenen Aufbewahrungszeit werden die gespeicherten Daten vom Ziel entfernt.

  Bei den Berechnungen der Aufbewahrungszeit wird davon ausgegangen, dass ein Monat 30 Tage und ein Jahr 365 Tage hat. Beispiel: Wenn Sie eine Aufbewahrungszeit von 2 Jahren, 2 Monaten und 5 Tagen festlegen, beläuft sich die gesamte Aufbewahrungszeit für Ihre kopierten Daten auf 795 Tage (365 + 365 + 30 + 30 + 5).

  Wichtig! Da diese Verweildauereinstellung sich nur auf Daten bezieht, die kopiert und von der Quelle zum Ziel verschoben worden sind (und nicht kopiert und aufbewahrt), ist es wichtig, sich dessen bewusst zu sein, dass nach Ablauf der angegebenen Aufbewahrungszeit, wenn die Daten vom Ziel entfernt werden, diese verschobenen Daten nicht mehr gespeichert werden.

- **Dateiversionen**: Diese Einstellung bezieht sich nur auf kopierte Daten, die aufbewahrt werden (nicht auf kopierte Daten, die verschoben werden).

  Gibt die Zahl der Kopien an, die aufbewahrt und am Zielspeicherort (Cloud oder Datenträger) gespeichert werden. Wenn diese Zahl überschritten wurde, wird die früheste (älteste) Version verworfen. Dieser Zyklus des Verwerfens der ältesten gespeicherten Version wiederholt sich jedes Mal, wenn neuere Versionen dem Ziel hinzugefügt werden, wodurch Sie immer die festgelegte Anzahl von gespeicherten Versionen aufbewahren können.

  Wenn Ihre festgelegte Anzahl an aufzubewahrenden Dateiversionen beispielsweise auf 5 festgelegt ist und Sie zu den Zeiten t1, t2, t3, t4 und t5 fünf Dateikopien ausführen, werden diese fünf Kopien die aufbewahrten und zur Wiederherstellung verfügbaren Dateikopieversionen. Nachdem die sechste Dateikopie ausgeführt wurde (neue Version wird gespeichert), entfernt CA ARCserve D2D die t1-Kopie und die fünf zur Wiederherstellung verfügbaren Versionen werden zu t2, t3, t4, t5 und t6.

  Standardmäßig beläuft sich die Zahl der vor der Beseitigung am Zielspeicherort aufbewahrten Dateien auf 15.

5. Klicken Sie auf "Einstellungen speichern".

Die Einstellungen für das Dateikopieziel wurden gespeichert.

Festlegen von Cloud-Konfigurations-Details für Dateikopie

In diesem Dialogfeld können Sie das Drop-down-Menü verwenden, um auszuwählen, welchen Cloud-Anbietertyp Sie für die Speicherung Ihrer Dateikopien verwenden möchten. Die verfügbaren Optionen sind Amazon S3, Windows Azure, Fujitsu-Cloud (Windows Azure) und Eucalyptus-Walrus. (Amazon S3 ist der Standardanbieter). Weitere Informationen zu Fujitsu-Cloud (Windows Azure) finden Sie unter Übersicht und Registrierung.

Hinweis: Wenn Sie Eucalyptus Walrus als Cloud-Anbieter für Ihre Dateikopie verwenden, können Sie Dateien kopieren, deren gesamte Pfadlänge größer ist als 170 Zeichen.

Die Konfigurationsoptionen für jeden Cloud-Anbieter sind ähnlich (mit etwas unterschiedlicher Terminologie), und alle Unterschiede werden beschrieben.

1. Festlegen der Verbindungseinstellungen

   Anbieter-URL:

   Identifiziert die URL-Adresse des Cloud-Anbieters.

   (Für Amazon S3, Windows Azure und Fujitsu-Cloud (Windows Azure) wird die Anbieter-URL automatisch aufgefüllt. Bei Eucalyptus-Walrus muss die Anbieter-URL mithilfe des angegebenen Formats manuell eingegeben werden).

Zugriffsschlüssel-ID/Kontoname/Abfrage-ID

Identifiziert den Benutzer, der Zugriff auf diesen Speicherort anfordert.

(Für dieses Feld verwendet Amazon S3 die Zugriffsschlüssel-ID, Windows Azure und Fujitsu-Cloud (Windows Azure) verwenden den Kontonamen, und Eucalyptus-Walrus verwendet die Abfrage-ID).

Geheimer Zugriffsschlüssel/Geheimschlüssel

Da Ihr Zugriffsschlüssel nicht verschlüsselt ist, stellt der geheime Zugriffsschlüssel ein Kennwort dar, das verwendet wird, um die Echtheit der Anfrage nach Zugriff auf diesen Speicherort zu überprüfen.

Wichtig! Der geheime Zugriffsschlüssel ist für die Gewährleistung der Sicherheit Ihrer Konten entscheidend. Sie sollten Ihre Schlüssel und Kontoanmeldeinformationen an einem sicheren Speicherort aufbewahren. Betten Sie Ihren geheimen Zugriffsschlüssel nicht auf einer Webseite oder einem anderen öffentlich zugreifbaren Quellcode ein, und übertragen Sie ihn nicht über unsichere Kanäle.

(Für dieses Feld verwendet Amazon S3 den geheimen Zugriffsschlüssel. Windows Azure, Fujitsu-Cloud (Windows Azure), und Eucalyptus-Walrus verwenden den geheimen Schlüssel).

Proxy aktivieren

Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Computernamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet. Sie können diese Option auch auswählen, wenn Ihr Proxy-Server Authentifizierung erfordert. Sie müssen dann die entsprechenden Authentifizierungsinformationen (Benutzername und Kennwort) angeben, die zur Verwendung des Proxy-Servers erforderlich sind.

(Proxy-Fähigkeit ist für Eucalyptus-Walrus nicht verfügbar).

2. Festlegen der erweiterten Einstellungen

Bucket-Name/Container

Alle Dateien und Ordner, die zum Cloud-Anbieter verschoben oder kopiert wurden, werden und in Ihren Buckets (oder Container) gespeichert und organisiert. Buckets sind wie Container für Ihre Dateien und werden verwendet, um Objekte zu gruppieren und zusammen zu organisieren. Alle Objekte, die beim Cloud-Anbieter gespeichert wurden, werden in einen Bucket abgelegt.

(Für dieses Feld verwenden Amazon S3 und Eucalyptus-Walrus "Bucket Name". Windows Azure und Fujitsu Cloud (Windows Azure) verwenden Container.

Hinweis: Für die restlichen Schritte können, soweit nicht anders angegeben, alle Verweise zu den Buckets auch auf die Container angewendet werden.

So geben Sie einen neuen Bucket-Namen an

a. Geben Sie Ihren neuen Bucket-Namen an.

   Hinweis: CA ARCserve Central Protection Manager erstellt den Bucket-Namen nicht, allerdings wird dieser für jeden CA ARCserve D2D-Knoten generiert, wenn ihm erfolgreich eine CA ARCserve Central Protection Manager-Richtlinie zugewiesen wird. Der Bucket-Name für jeden CA ARCserve D2D-Knoten erhält automatisch den Namen "d2dfilecopy-<Hostname>-<vom Benutzer erteileter Name>" als Präfix.

   Ein Bucket-Name sollte einmalig, leicht identifizierbar und mit den Benennungsregeln für Internet-Domänen kompatibel sein. Zwei Buckets dürfen nicht den gleichen Namen haben. Es ist wichtig, die gültige Syntax für Bucket-Namen zu kennen.

   In der Amazon S3-Dokumentation finden Sie weitere Informationen über die Namensanforderungen von Buckets für Amazon S3 und Eucalyptus-Walrus.

   In der Microsoft-Dokumentation finden Sie weitere Informationen über die Namensanforderungen von Containern für Windows Azure und Fujitsu Cloud (Windows Azure).

b. Wählen Sie nur für Amazon S3 eine verfügbare Region aus dem Drop-down-Menü aus. Standardmäßig sind alle verfügbaren Regionen im Drop-down-Menü enthalten und Sie können die Region auswählen, in der neue Bucket erstellt werden soll.

   Regionen ermöglichen es Ihnen, die geografische Region zu wählen, in der Amazon S3 Buckets speichert, die Sie erstellen. Wählen Sie eine Region aus, die Ihnen schnellen Zugriff auf Ihre Daten bietet und es Ihnen erlaubt, Wartezeiten zu optimieren, Kosten zu minimieren oder sich mit gesetzlichen Vorschriften zu befassen.

   (Bei Windows Azure, Fujitsu Cloud (Windows Azure) und Eucalyptus-Walrus kann die Region nicht ausgewählt werden).

c. Nachdem Sie Ihre Werte ausgewählt haben, klicken Sie auf OK. Der Bucket-Name wird validiert und auf der Cloud erstellt.

d. Wenn Sie den neuen Bucket erfolgreich erstellt haben, gelangen Sie zum Hauptdialogfeld "Cloud-Konfiguration", und die neuen Bucket-Informationen (Name und Region) werden in den Feldern "Erweiterte Einstellungen" angezeigt.

"Reduced Redundancy Storage" aktivieren

Nur bei Amazon S3 können Sie mit dieser Option "Reduced Redundancy Storage" (RRS) aktivieren. RRS ist eine Speicherungsoption von Amazon S3, mit der Sie Kosten reduzieren können, indem Sie nicht kritische, reproduzierbare Daten auf geringeren Redundanz-Ebenen als der Standardspeicher von Amazon S3 speichern. Sowohl die standardmäßigen Optionen als auch die Speicheroptionen zur reduzierten Redundanz speichern Daten in mehreren Einrichtungen und auf mehreren Geräten. Allerdings werden mit RRS die Daten weniger repliziert, sodass die Kosten geringer sind. Sie sollten die gleiche Latenz und den gleichen Durchsatz erhalten, indem Sie entweder den Standardspeicher von Amazon S3 oder RRS verwenden. Standardmäßig ist diese Option nicht aktiviert (Amazon S3 verwendet die standardmäßige Speicheroption).

3. Klicken Sie auf "Verbindung testen", um die Verbindung zum angegebenen Cloud-Speicherort zu überprüfen.

4. Klicken Sie auf "OK", um das Dialogfeld "Cloud-Konfiguration" zu verlassen.

Festlegen der Dateikopieablaufpläne

Mit CA ARCserve Central Protection Manager können Sie die Ablaufplaneinstellungen für die Informationen angeben, die kopiert werden sollen.

So legen Sie Dateikopieablaufpläne fest

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

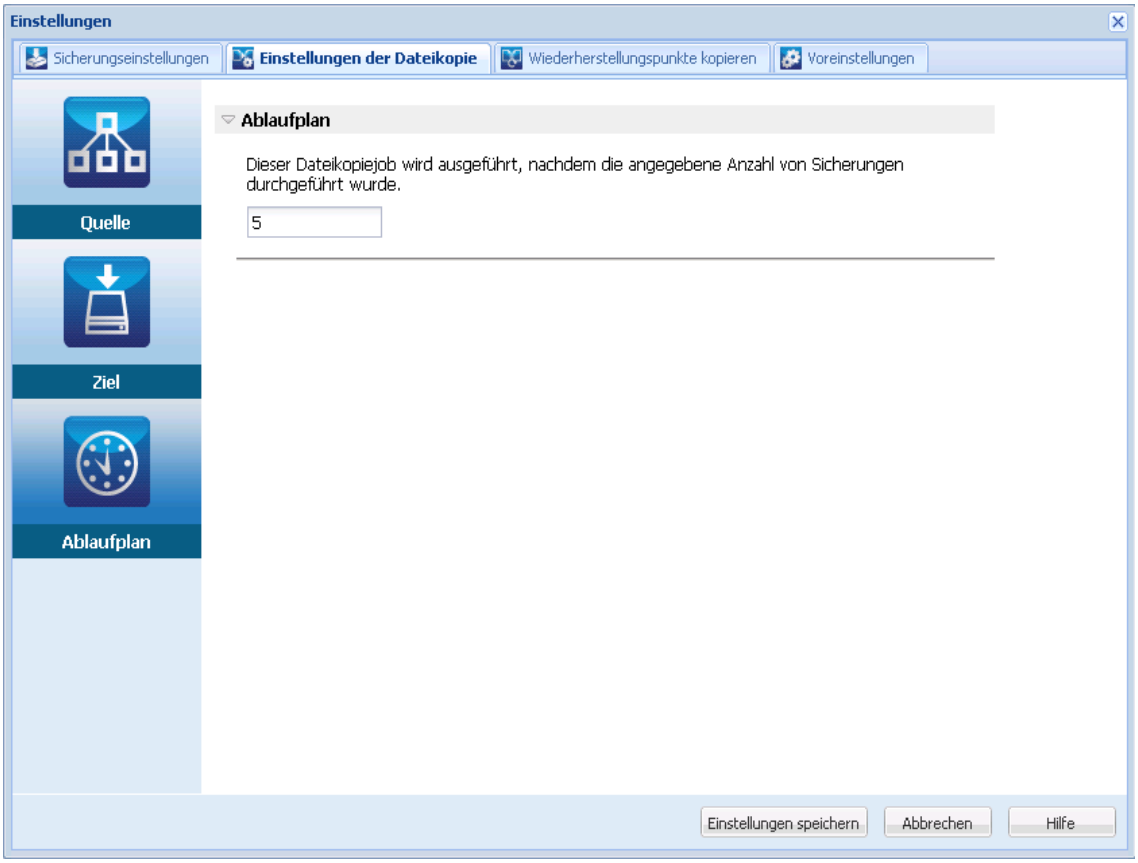
   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Wählen Sie die Registerkarte "Dateikopieeinstellungen" aus und wählen Sie dann "Ablaufplan".

   Das Dialogfeld für den Ablaufplan der Einstellungen der Dateikopie öffnet sich.



4. Legen Sie die Einstellungen für Ihren Dateikopieablaufplan fest.

   - **Ablaufplan**: Aktiviert die Dateikopie von Daten nach der festgelegten Anzahl von Sicherungen.

     Der Dateikopierprozess wird automatisch nach der angegebenen Anzahl von erfolgreichen Sicherungen gestartet und basiert auf den von Ihnen ausgewählten Dateikopierrichtlinien.

     Sie können diese Einstellung verwenden, um zu kontrollieren, wie oft ein Dateikopierjob am Tag ausgelöst wird. Wenn Sie beispielsweise festlegen, dass ein Sicherungsjob alle 15 Minuten ausgeführt werden soll, werden, falls Sie angeben, dass ein Dateikopierjob nach jeder vierten Sicherung ausgeführt werden soll, 24 Dateikopier-Archivierungen am Tag stattfinden (eine pro Stunde).

     Standardmäßig sieht der Ablaufplan eine Dateikopie nach jeder fünften erfolgreich abgeschlossenen Sicherung vor. (Die maximale Anzahl von Sicherungen, die festgelegt werden können, ist 700).

5. Klicken Sie auf "Einstellungen speichern".

Die Einstellungen für das Dateikopieablaufplan wurden gespeichert.

Festlegen der Einstellungen für das Kopieren von Wiederherstellungspunkten

Mit CA ARCserve D2D können Sie die Ablaufplaneinstellungen für Ihre zu kopierenden (und bei Bedarf zu exportierenden) Wiederherstellungspunkte festlegen. Ein besseres Verständnis darüber, wie die Optionen auf diesem Dialogfeld verwendet werden können, um Ihren Ablaufplan für das Kopieren von Wiederherstellungspunkten zu konfigurieren, erhalten Sie unter Kopieren von Wiederherstellungspunkten - Beispielszenarien.

Hinweis: Das Kopieren von Wiederherstellungspunkten ist ein Kopier- und Einfügevorgang und kein Ausschneide- und Einfügevorgang. Jedes Mal wenn ein geplanter Kopiervorgang von Wiederherstellungspunkten ausgeführt wird, erstellt CA ARCserve D2D daher eine zusätzliche Kopie des Wiederherstellungspunkts im angegebenen Kopierziel, während es die ursprüngliche Kopie des Wiederherstellungspunkts in dem Sicherungsziel behält, das in den Sicherungseinstellungen festgelegt wurde.

So legen Sie die Einstellungen für das Kopieren von Wiederherstellungspunkten fest

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

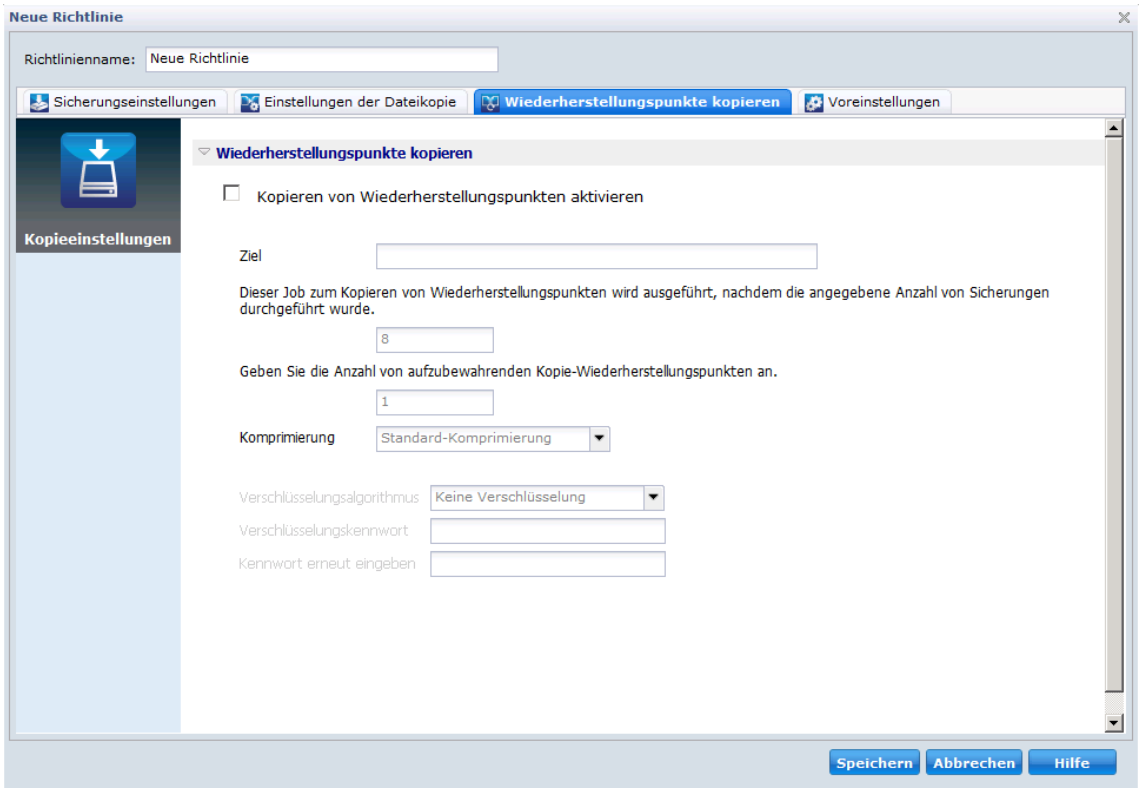
   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Wählen Sie die Registerkarte "Wiederherstellungspunkte kopieren" aus.

   Das Dialogfeld "Wiederherstellungspunkte kopieren" wird angezeigt.



4. Festlegen der Einstellungen des Ablaufplans für die Kopie von Wiederherstellungspunkten

Aktivieren des Kopierens von Wiederherstellungspunkten

Aktiviert die geplanten Kopien von Wiederherstellungspunkten nach der festgelegten Anzahl von Sicherungen. Wenn Sie diese Option nicht aktiviert ist, wird keine geplante Kopie von Wiederherstellungspunkten ausgeführt.

Ziel

Legt den Speicherort (das Ziel) für die Kopien der Wiederherstellungspunkte fest. Sie können auch nach einem Speicherort durchsuchen. Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen.

Dieser Job zum Kopieren von Wiederherstellungspunkten wird ausgeführt, nachdem die angegebene Anzahl von Sicherungen durchgeführt wurde.

Legt fest, wann der geplante Kopiervorgang der Wiederherstellungspunkte automatisch gestartet wird.

Der Kopiervorgang von Wiederherstellungspunkten wird nach der angegebenen Anzahl von erfolgreichen Sicherungen automatisch gestartet und basiert auf den von Ihnen ausgewählten Kopierrichtlinien.

Sie können diese Einstellung verwenden, um zu kontrollieren, wie oft ein Kopiervorgang von Wiederherstellungspunkten am Tag ausgelöst wird. Wenn Sie beispielsweise festlegen, dass ein Sicherungsjob alle 15 Minuten ausgeführt wird, und die Wiederherstellungspunkte nach jeder vierten Sicherung kopiert werden, werden 24 Kopierjobs von Wiederherstellungspunkten am Tag ausgeführt (einer pro Stunde).

Standardmäßig sieht der Ablaufplan das Kopieren von Wiederherstellungspunkten nach jeder achten erfolgreich abgeschlossenen Sicherung vor.

Wichtig! Wenn Sie Sicherungs- und Kopierjobs so planen, dass sie in regelmäßigen Intervallen ausgeführt werden, und der Kopierjob gerade zu dem Zeitpunkt ausgeführt wird (in aktivem Status ist), für den der Sicherungsjob geplant ist, schlägt der Sicherungsjob fehl. (Der nächste Sicherungsjob wird wie geplant ausgeführt und sollte erfolgreich sein, wenn er nicht mit einem anderen Kopierjob im Konflikt steht). Da der Kopiervorgang fast die gleiche Zeit in Anspruch nimmt wie die Ausführung einer vollständigen Sicherung, wird empfohlen, den Ablaufplan nicht auf häufige Kopierjobs für Ihre Wiederherstellungspunkte festzulegen.

Geben Sie die Anzahl von aufzubewahrenden Kopie-Wiederherstellungspunkten an.

Legt die Anzahl von Wiederherstellungspunkten fest, die aufbewahrt und am angegebenen Kopierziel gespeichert werden. Wenn diese Zahl überschritten wurde, wird der früheste (älteste) Wiederherstellungspunkt verworfen. Dieser Zyklus des Verwerfens der ältesten gespeicherten Wiederherstellungspunkte wiederholt sich jedes Mal, wenn neuere Versionen dem Ziel hinzugefügt werden, wodurch Sie immer die festgelegte Anzahl an gespeicherten Wiederherstellungspunkte aufbewahren können.

Hinweis: Wenn auf Ihrem Ziel nicht genügend freier Speicherplatz zur Verfügung steht, sollten Sie in Betracht ziehen, die Anzahl der gespeicherten Wiederherstellungspunkte zu reduzieren.

Standardmäßig ist eine Verweildauer von 31 Wiederherstellungspunkten festgelegt.

Hinweis: Die Höchstanzahl der Wiederherstellungspunkte liegt bei 1344.

Komprimierung

Legt den Komprimierungstyp fest, der für das Kopieren der Wiederherstellungspunkte verwendet werden soll.

Eine Komprimierung wird normalerweise durchgeführt, um den verwendeten Speicherplatz zu verringern, hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit der Sicherung.

Es sind folgende Optionen verfügbar:

- **Keine Komprimierung**: Es wird keine Komprimierung durchgeführt. Die Dateien sind reine VHD-Dateien. Diese Option bedeutet niedrigste CPU-Auslastung (höchste Geschwindigkeit), aber auch höchste Speicherplatzverwendung für Ihr Sicherungs-Image.
- **Keine Komprimierung - VHD**: Es wird keine Komprimierung durchgeführt. Die Dateien werden direkt in .VHD-Format konvertiert, ohne manuell vorgehen zu müssen. Diese Option bedeutet niedrigste CPU-Auslastung (höchste Geschwindigkeit), aber auch höchste Speicherplatzverwendung für Ihr Sicherungs-Image.
- **Standard-Komprimierung**: Komprimierung wird bis zu einem gewissen Grad durchgeführt. Diese Option bietet ein Gleichgewicht zwischen CPU-Auslastung und verwendetem Speicherplatz. Diese Einstellung ist die Standardeinstellung.
- **Maximale Komprimierung**: Es wird eine maximale Komprimierung durchgeführt. Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigste Speicherplatzverwendung für Ihr Sicherungs-Image.

Hinweis: Wenn Ihr Sicherungs-Image unkomprimierbare Daten enthält (wie JPG-Images oder ZIP-Dateien), kann zusätzlicher Speicherplatz zugewiesen werden, um diese Art von Daten zu verarbeiten. Die Aktivierung einer Komprimierungs-Option und das Vorhandensein unkomprimierbarer Daten in Ihrer Sicherung kann in solchen Fällen eine erhöhte Speicherplatzverwendung zur Folge haben.

Verschlüsselungsalgorithmus

Legt den Typ des für das Kopieren der Wiederherstellungspunkte zu verwendenden Verschlüsselungsalgorithmus fest.

Bei der Datenverschlüsselung werden Daten in ein Format umgewandelt, das ohne den entsprechenden Entschlüsselungsmechanismus nicht verständlich ist. Der Datenschutz von CA ARCserve D2D verwendet sichere AES- (Advanced Encryption Standard) Verschlüsselungsalgorithmen, um maximale Sicherheit und Datenschutz Ihrer angegebenen Daten zu erreichen.

Die verfügbaren Formatoptionen sind "Keine Verschlüsselung", "AES-128", "AES-192" und "AES-256". (Um die Verschlüsselung zu deaktivieren, wählen Sie "Keine Verschlüsselung" aus).

Verschlüsselungskennwort

Wenn der zu kopierende Wiederherstellungspunkt zuvor verschlüsselt wurde, müssen Sie das Kennwort angeben (und bestätigen).

- Wenn der Wiederherstellungspunkt an einem Speicherort auf dem gleichen Rechner kopiert wird, wird das Verschlüsselungskennwort gespeichert und dieses Feld wird automatisch aufgefüllt.
- Wenn der Wiederherstellungspunkt auf einem anderen Rechner kopiert wird, müssen Sie das Verschlüsselungskennwort eingeben.

5. Klicken Sie auf "Einstellungen speichern".

Die Einstellungen für das Kopieren von Wiederherstellungspunkten werden gespeichert.

Verwalten von Voreinstellungen

CA ARCserve Central Protection Manager ermöglicht die Verwaltung der allgemeinen Anforderungen einer Richtlinie. Sie können Nachrichten-Feeds generieren, E-Mail-Warnmeldungen erstellen oder Ihren Server bzw. Ihre Verbindungen aktualisieren.

Dieser Abschnitt enthält folgende Themen:

Festlegen der allgemeinen Voreinstellungen (siehe Seite 125)
Festlegen der E-Mail-Warnmeldungen (siehe Seite 127)
Festlegen der Voreinstellungen für Aktualisierungen (siehe Seite 133)

Festlegen der allgemeinen Voreinstellungen

CA ARCserve Central Protection Manager ermöglicht das Festlegen der allgemeinen Voreinstellungen einer Richtlinie.

So legen Sie allgemeine Voreinstellungen fest

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

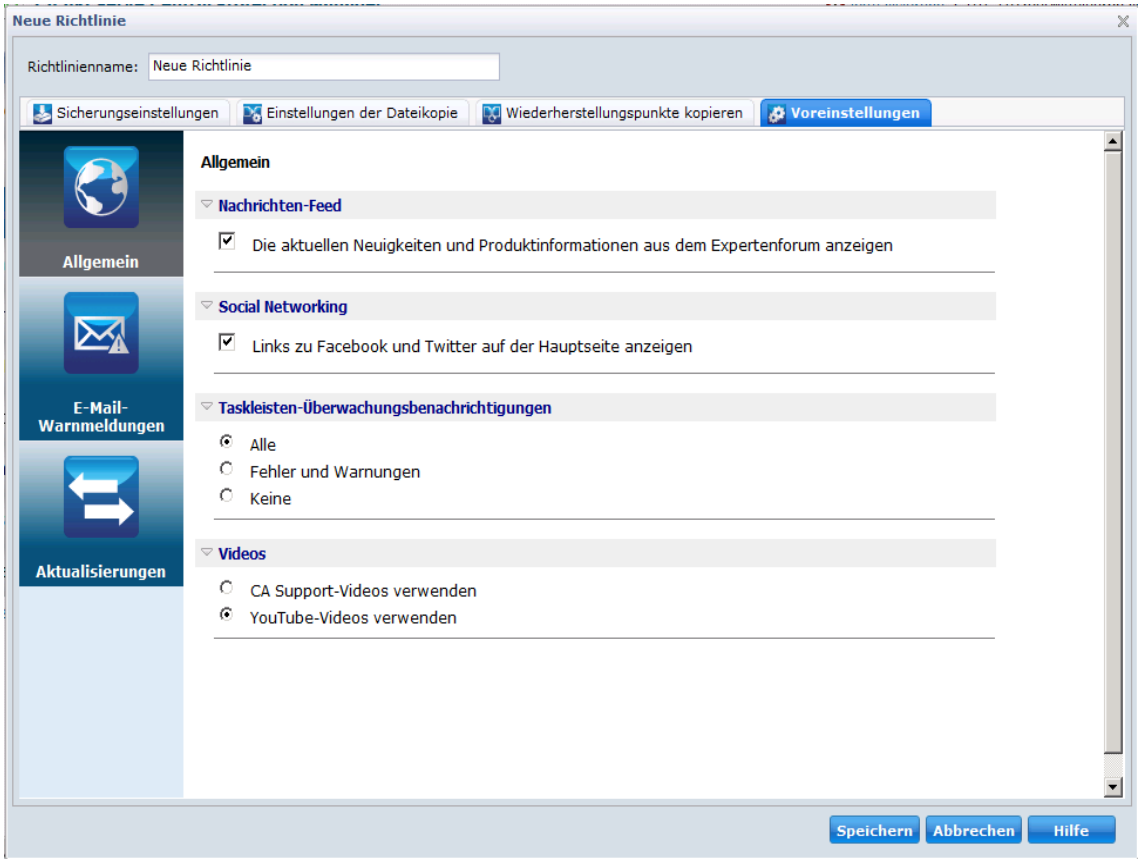
   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Wählen Sie die Registerkarte "Voreinstellungen" aus.

   Das Dialogfeld "Allgemeine Einstellungen" wird geöffnet.



4. Festlegen Ihrer Voreinstellungen
   - **Nachrichten-Feed**: Aktivieren Sie diese Option, um die aktuellsten Nachrichten und Produktinformationen aus dem Expertenforum anzuzeigen.
   - **Social Networking**: Aktivieren Sie diese Option, um Verknüpfungen zu Facebook und Twitter von der Hauptseite anzuzeigen.
   - **Taskleistenbenachrichtigungen**: Sie können zwischen den folgenden Optionen wählen:
     - Wählen Sie "Alle" aus, um alle Benachrichtigungen in Ihrer Taskleiste anzuzeigen.
     - Wählen Sie "Fehler und Warnungen" aus, um nur Fehler und Warnungen in Ihrer Taskleiste anzuzeigen.
     - Wählen Sie "Keine" aus, um keine Benachrichtigungen anzuzeigen.
   - **Videos**: Wählen Sie einen in Ihrer D2D-Richtlinie zu verwendenden Videotyp aus:
     - CA Support-Videos verwenden
     - YouTube-Videos verwenden (Standard)
5. Klicken Sie auf "Speichern".

Die allgemeine Voreinstellungen werden gespeichert.

Festlegen der E-Mail-Warnmeldungen

In CA ARCserve Central Protection Manager können Sie Voreinstellungen für E-Mail-Warnungen festlegen.

So legen Sie E-Mail-Warnungen fest

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

   Der Richtlinienbildschirm wird angezeigt.
2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Wählen Sie die Registerkarte "Voreinstellungen" und danach "E-Mail-Warnungen" aus.

   Das Dialogfeld "E-Mail-Warnmeldungen" der Voreinstellungen wird geöffnet.

4. Legen Sie Ihre E-Mail-Warnmeldungen fest.

   - **E-Mail-Warnmeldungen aktivieren**: Wählen Sie diese Option aus, um die Voreinstellungen auf diesem Fenster zu aktivieren.
   - **E-Mail-Einstellungen**: Klicken Sie auf diese Schaltfläche, um das Dialogfeld E-Mail-Einstellungen (siehe Seite 131) zu öffnen.
   - **Benachrichtigungen**: Legt automatische E-Mail-Benachrichtigungen über den Status ausgewählter Ereignisse fest. Sie können jede beliebige oder alle der verfügbaren Optionen auswählen.

     Die verfügbaren Optionen bieten Warnmeldungen für die folgenden Ereignisse:

     Warnmeldungen zu Sicherungsjobs

     - **Versäumte Jobs**: Sendet eine E-Mail-Warnmeldung für alle versäumten Jobs. Ein versäumter Job ist ein geplanter Job, der nicht zum geplanten Zeitpunkt ausgeführt wurde. Dies kann vorkommen, wenn ein anderer Job ausgeführt wird oder ein vorhergehender, früher gestarteter Job noch nicht beendet ist. Wenn zum Beispiel ein Export- oder Wiederherstellungsjob zum für den Sicherungsjob geplanten Zeitpunkt ausgeführt wird, wird dieser Sicherungsjob versäumt.
     - **Sicherung, Katalog, Dateikopie, Wiederherstellung oder Kopieren von Wiederherstellungspunkten schlägt fehl oder stürzt ab**: Sendet eine Warnmeldung per E-Mail für jede nicht erfolgreiche Sicherung, Katalog, Dateikopie, Wiederherstellung oder Kopie von Wiederherstellungspunkten. Diese Kategorie schließt alle fehlgeschlagenen, unvollständigen, abgebrochenen, versäumten und abgestürzten Versuche mit ein.
     - **Sicherung, Katalog, Dateikopie, Wiederherstellung oder Kopieren von Wiederherstellungspunkten ist erfolgreich**: Sendet eine Warnmeldung per E-Mail für jede erfolgreiche Sicherung, Katalog, Dateikopie, Wiederherstellung oder Kopie von Wiederherstellungspunkten.
     - **Der Zusammenführungsjob wurde angehalten, übersprungen, schlug fehl oder ist abgestürzt:** Sendet eine Alert-Benachrichtigung für alle Zusammenführungsjob, die angehalten, übersprungen, fehlgeschlagen oder abgestürzt sind. Wenn Sie diese Warnmeldung aktivieren, werden Sie informiert, sobald eine Zusammenführung fehlschlägt. Ein Zusammenführungsfehler kann aus den folgenden Gründen auftreten: die Sitzung wird geladen, die Sitzung wird von einem Katalogjob gesperrt, oder die Sitzung wird aufgrund anderer Gründe gesperrt.
     - **Zusammenführungsjob erfolgreich:** Sendet eine Warnmeldung für alle erfolgreichen Zusammenführungsjobs.

Warnmeldungen zu Speicherplatz

- **Freier Speicher am Sicherungsziel liegt unter dem Wert**: Sendet eine Warnmeldung per E-Mail, wenn der erforderliche Speicherplatz am Sicherungsziel unter dem angegebenen Wert liegt. Sie können außerdem entweder einen Prozentsatz der Gesamtkapazität oder einen bestimmten Wert (in MB) festlegen, bei dessen Übertreten eine Warnmeldung versendet werden soll.

Warnmeldungen zu Aktualisierungen

- **Neue Aktualisierung verfügbar**: Sendet eine Benachrichtigung per E-Mail, wenn neue Aktualisierungen für CA ARCserve D2D verfügbar sind. E-Mail-Benachrichtigungen werden auch gesendet, wenn ein Fehler während der Überprüfung auf Aktualisierungen oder des Downloads auftritt.

Warnmeldungen zu Ressourcen

- **Aktivieren von Warnmeldungen zu Ressourcen**: Sendet eine Benachrichtigung per E-Mail, wenn eine Schwellenwertebene für eine angegebene Leistungskennzahl (PKI) erreicht wird. Um sicherzustellen, dass Ihr Server effizient und zuverlässig arbeitet, müssen Sie die Leistung ständig überwachen, um mögliche Probleme zu identifizieren und rasch auf Engpasssituationen zu reagieren.

  Das Festlegen von Schwellenwerten für diese Leistungsindikatoren liegt ganz bei Ihnen und hängt von Ihren Kenntnissen des Servers ab. Es gibt keine richtigen oder falschen Einstellungen. Diese Alert-Benachrichtigungen sollten auf "normaler" und annehmbarer Leistung basieren. Wenn die CPU-Auslastung Ihres Systems zum Beispiel bei 80 % liegt, wäre es nicht sehr nützlich oder effizient, den Schwellenwert der CPU-Auslastung auf 75 % festzulegen.

  Jeder dieser PKI-Parameter kann separat konfiguriert werden, um eine Warnmeldung zu senden, wenn der entsprechende Schwellenwert erreicht wird. Es können maximal 5 E-Mails pro Tag zum PKI-Alert gesendet werden.

- **CPU-Auslastung**: Der angegebene Alert-Schwellenwert der CPU-Auslastung zeigt den Prozentsatz der CPU-Auslastung für Ihren durch CA ARCserve D2D geschützten Server an. Sie können diese Alert-Benachrichtigung verwenden, um sicher zu stellen, dass Ihr Server nicht zu oft überladen wird.

  Wenn die CPU-Auslastung zu hoch ist, kann die Serverantwortzeit sehr groß werden oder der Server reagiert möglicherweise überhaupt nicht mehr, und Sie sollten in Betracht ziehen, die Last besser (bzw. gleichmäßig) zu verteilen.

- **Datenträgerdurchsatz:** Der angegebene Alert-Schwellenwert des Datenträgerdurchsatzes zeigt den Datenträgerdurchsatz (MB/Sekunde) für Ihren durch CA ARCserve D2D geschützten Server an. Sie können diese Alert-Benachrichtigung verwenden, um sicher zu stellen, dass Sie die Kapazitäten Ihres Datenträgers maximieren.

  Wenn Ihr Festplattendurchsatz nahe bei dem Maximalwert liegt, den Ihre Festplatte verarbeiten kann, sollten Sie ein Upgrade auf eine Festplatte in Betracht ziehen, die Ihren Anforderungen besser entspricht. Im Allgemeinen führt eine schnellere Festplatte zu einer höheren Leistung.

- **Arbeitsspeichernutzung**: Der angegebene Alert-Schwellenwert der Arbeitsspeichernutzung zeigt den Prozentsatz des verwendeten Speichers auf Ihrem durch CA ARCserve D2D geschützten Server an. "Nutzung" bedeutet, wie viel Ihrer Speicherkapazität Sie verwenden. Je höher der Prozentsatz, desto geringer Ihre Serverleistung.

  Wenn Ihre Speichernutzung ständig zu hoch ist, müssen Sie herausfinden, welcher Prozess diese hohe Nutzung verursacht. Sie können diese Indikatoreinstellung verwenden, um Sie darauf hinzuweisen, wenn für eine Anwendung oder einen Server ein Upgrade notwenig sein könnte.

- **Netzwerk-E/A**: Der angegebene Alert-Schwellenwert des Netzwerk-E/A zeigt den Prozentsatz NIC-Bandbreite an, die momentan auf Ihrem durch CA ARCserve D2D geschützten Server verwendet wird. "Auslastung" bedeutet, in welchem Maße Ihre Netzwerkkarten (oder NIC) ausgelastet sind. Je höher der Prozentsatz, desto geringer Ihre Netzwerkleistung.

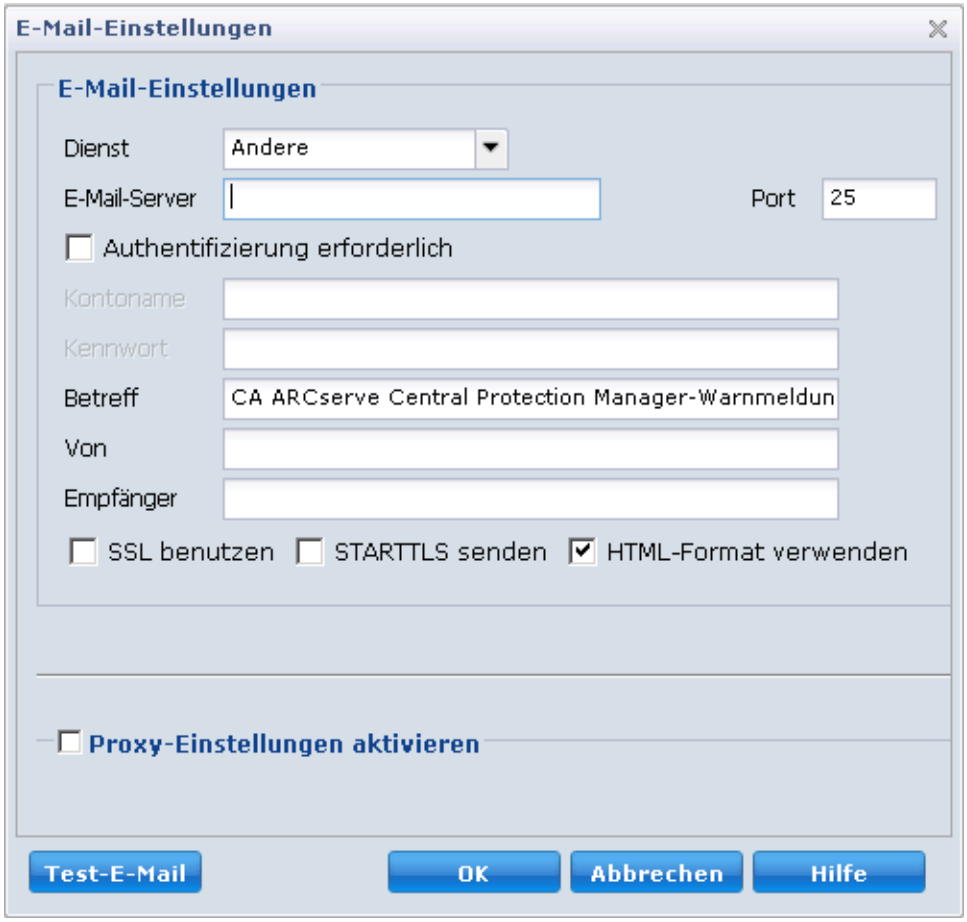
  Wenn Ihre Netzwerkauslastung ständig zu hoch ist, müssen Sie herausfinden, welcher Prozess diese hohe Nutzung verursacht, und das Problem beheben. Wenn der Prozentsatz der Netzwerkauslastung auf der Basis Ihrer Netzwerkkapazität während der Sicherung zu hoch, müssen Sie möglicherweise Ihre Netzwerkkarte aufrüsten, um die höheren Durchsatzanforderungen zu erfüllen.

5. Klicken Sie auf "Speichern".

Die Alert-E-Mail-Optionen werden gespeichert.

Festlegen der E-Mail-Einstellungen

Das Dialogfeld "E-Mail-Einstellungen" füllt automatisch die aktuellen Werte des E-Mail-Servers und der Richtlinien-E-Mail-Konfiguration in der neuen Richtlinie auf. Diese Einstellungen werden für alle Warnmeldungen per E-Mail verwendet. Sie können jederzeit geändert werden.



Dienst

E-Mail-Provider, der für das Versenden der Warnmeldungen verwendet werden soll. Die verfügbaren Optionen sind "Google Mail", "Yahoo Mail", "Live Mail" und "Andere".

- Wenn Sie "Andere" auswählen, müssen Sie den zu verwendenden E-Mail-Server und die entsprechende Portnummer angeben, die standardmäßig festgelegt sind.
- Wenn Sie "Google Mail", "Yahoo Mail" oder "Live Mail" auswählen, werden die Felder "E-Mail-Server" und "Portnummer" automatisch aufgefüllt.

Mailserver

Hostname des SMTP-Mailservers, den CA ARCserve D2D zur Versendung von Warnmeldungen per E-Mail verwendet.

Port

Ausgabeportnummer für den Mail-Server.

Authentifizierung erforderlich

Gibt an, ob für eine Authentifizierung für diesen Mail-Server erforderlich ist, um eine E-Mail per Internet zu senden. Wenn diese Option ausgewählt ist, müssen der entsprechende Kontoname und das entsprechende Kennwort angegeben werden.

Betreff

Beschreibung der Warnmeldungen, die CA ARCserve D2D per E-Mail versendet. Standardmäßig wird "CA ARCserve D2D-Warnmeldung" verwendet.

Von

Die E-Mail-Adresse, die CA ARCserve D2D für das Versenden von Warnmeldungen per E-Mail verwendet.

Empfänger

E-Mail-Adresse der Empfänger der Warnmeldungen per E-Mail.

Hinweis: Trennen Sie bei der Eingabe mehrerer E-Mail-Adressen die einzelnen Adressen durch ein Semikolon.

Geöffnete Dateien mit SSL sichern

Der E-Mail-Server benötigt zur sicheren Datenübertragung über das Internet eine SSL-Verbindung (Secure Sockets Layer).

STARTTLS senden

Der E-Mail-Server benötigt für den Aufbau einer sicheren SMTP-Verbindung einen STARTTLS-Befehl (Start TLS extension).

HTML-Format verwenden

Warnmeldungen per E-Mail werden als HTML gesendet. Wenn diese Option nicht ausgewählt ist, werden die Warnmeldungen in unformatiertem Textformat versendet. Standardmäßig ist diese Option aktiviert.

Proxy-Einstellungen aktivieren

Legt fest, ob für das Versenden der Warnmeldungen per E-Mail eine Verbindung zu einem Proxy-Server aufgebaut werden soll. Wenn diese Option ausgewählt wird, müssen Name und Portnummer des Proxy-Servers angegeben werden.

Test-E-Mail

Überprüft, ob die Einstellungen der E-Mail-Konfiguration richtig sind.

Festlegen der Voreinstellungen für Aktualisierungen

Mit CA ARCserve Central Protection Manager können Sie Ihre Voreinstellungen für die Aktualisierung festlegen.

So aktualisieren Sie allgemeine Voreinstellungen

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

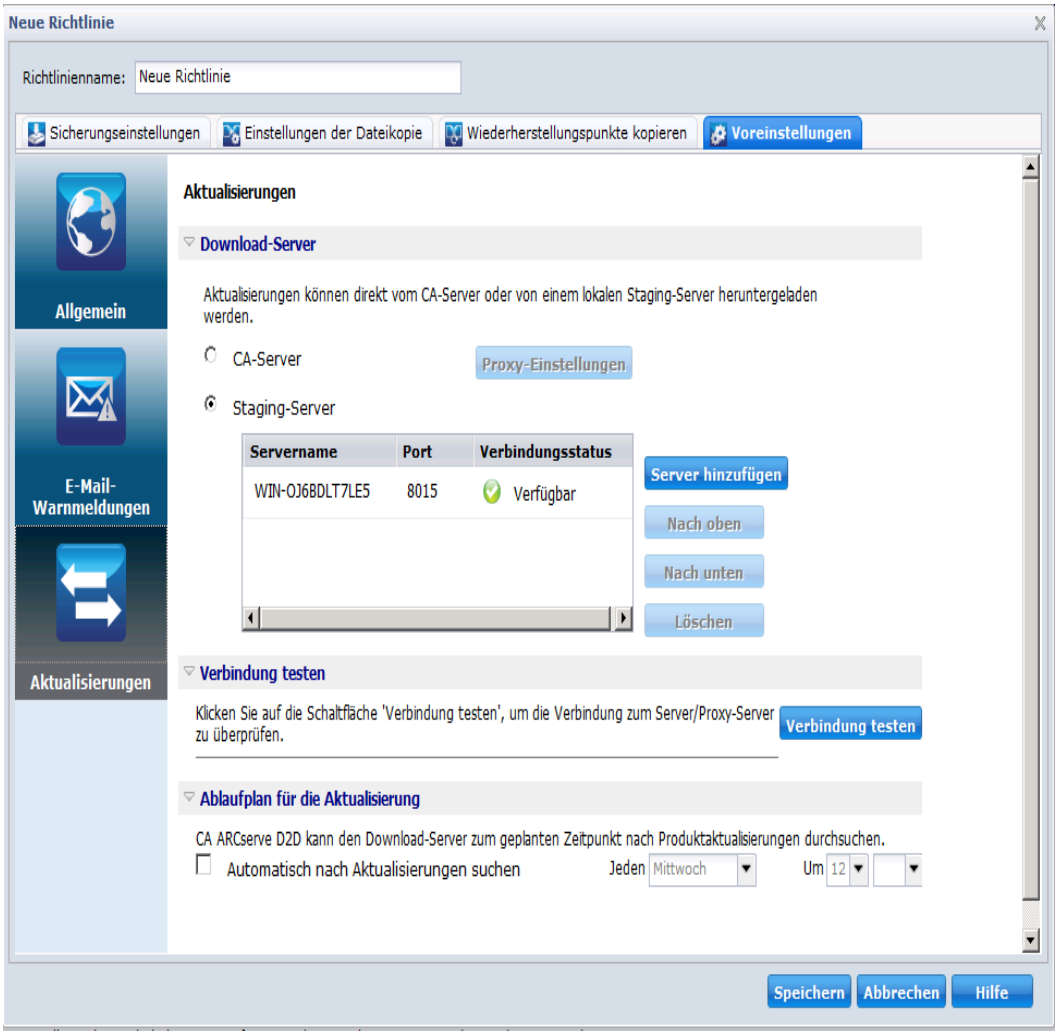
   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie auf "Neu", um eine neue Richtlinie zu erstellen.

   Das Dialogfeld "Neue Richtlinie" wird geöffnet.

3. Wählen Sie die Registerkarte "Voreinstellungen" und danach "Aktualisierung" aus.

   Das Dialogfeld "Aktualisierung" der Voreinstellungen wird geöffnet.



4. Festlegen der Voreinstellungen der Aktualisierung

   - **Download-Server**: Gibt den Quellserver an, von dem Ihr CA ARCserve D2D-Server aus eine Verbindung herstellt und verfügbare Aktualisierungen herunterlädt.

     - **CA Technologies-Server**: Mit dieser Option können Sie festlegen, dass CA ARCserve D2D-Aktualisierungen vom CA Technologies-Server direkt auf Ihren lokalen Server heruntergeladen werden.

     - **Staging-Server**: Mit dieser Option können Sie den Server festlegen, den Sie als Staging-Server verwenden möchten.

       Wenn Sie mehr als einen Staging-Server angeben, wird der erste aufgelistete Server als primärer Staging-Server festgelegt. CA ARCserve D2D versucht zuerst, mit dem primären Staging-Server Verbindung aufzunehmen. Wenn aus irgendeinem Grund der erste aufgelistete Server nicht verfügbar ist, wird der nächste aufgelistete Server als primärer Staging-Server verwendet. Mit dem gleichen Ablauf wird fortgefahren, bis der letzte aufgelistete Server der primäre Staging-Server wird. (Die Liste der Staging-Server ist auf maximal fünf Server beschränkt).

     - Sie können die Reihenfolge der Staging-Server mit den Schaltflächen "Nach unten" und "Nach oben" ändern.

     - Sie können die Schaltfläche "Löschen" verwenden, um einen Server aus dieser Auflistung zu entfernen.

     - Sie können die Schaltfläche "Server hinzufügen" verwenden, um einen neuen Server zur Auflistung hinzuzufügen. Wenn Sie auf die Schaltfläche "Server hinzufügen" klicken, öffnet sich das Dialogfeld "Staging-Server". Dort können Sie den Namen des hinzugefügten Staging-Servers und die Portnummer angeben, die standardmäßig der Nummer Ihres derzeitigen Ports entspricht.

       Dies ist die Standardeinstellung.

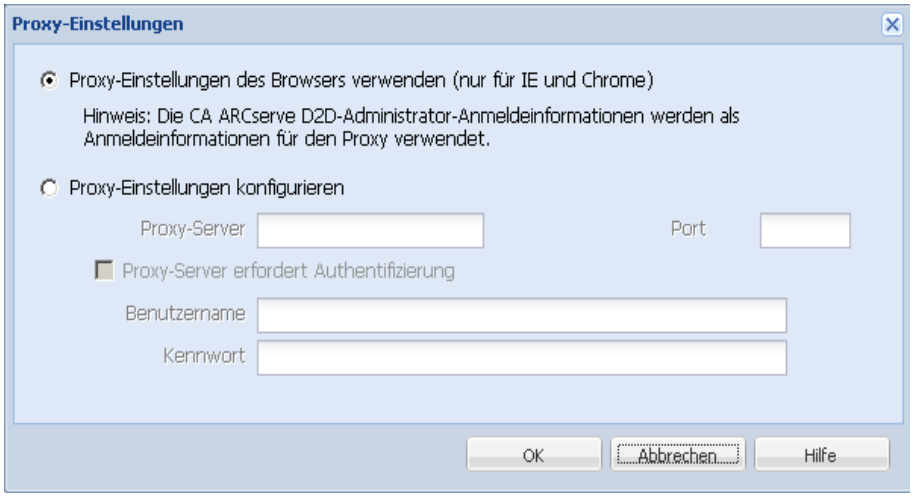
       Hinweis: Für D2D-Richtlinien ist der standardmäßige Staging-Server der lokale CA ARCserve Central Applications-Computer.

       CA ARCserve D2D-Aktualisierungen werden vom CA Technologies-Server direkt in das angegebene Verzeichnis des Staging-Servers heruntergeladen. Nachdem die Aktualisierungen auf diesen Staging-Server heruntergeladen wurden, können Sie anschließend Aktualisierungen vom Staging-Server auf einen Client-Server herunterladen. Wenn Sie das Verzeichnis des Staging-Servers auswählen, müssen Sie auch den Hostnamen und die IP-Adresse für den Staging-Server sowie die entsprechende Portnummer angeben.

- **Proxy-Einstellungen**: Diese Option ist nur verfügbar, wenn Sie "CA-Server" als den Download-Server auswählen.

  Wählen Sie die "Proxy-Einstellungen" aus, um anzugeben, ob die CA ARCserve D2D-Aktualisierungen über einen Proxy-Server heruntergeladen werden sollen. Dies wird die Verbindung zum CA-Server sein, von dem Ihr Download-Server die Aktualisierungen erhält.

  Wenn Sie auf diese Schaltfläche klicken, wird das Dialogfeld "Proxy-Einstellungen" geöffnet.



  - **Proxy-Einstellungen des Browsers verwenden (nur für IE und Chrome)**: Lässt Sie die Anmeldeinformationen verwenden, die für den CA ARCserve D2D-Proxy vorbereitet wurden.
  - **Proxy-Einstellungen konfigurieren**: Ein Proxy-Server fungiert als Schnittstelle zwischen Ihrem Download-Server (Staging oder Client) und dem CA-Server, um Sicherheit, erhöhte Leistung und administrative Berechtigungen sicherzustellen. Standardmäßig ist diese Option deaktiviert.

    Wenn diese Option ausgewählt ist, wird ein Proxy-Server verwendet, um eine Verbindung zum CA-Server für CA ARCserve D2D-Aktualisierungsinformationen herzustellen. Der Proxy-Server stellt eine direkte Verbindung zum CA-Server her, um Aktualisierungsinformationen zu erhalten. Wenn Sie diese Option auswählen, müssen Sie auch die IP-Adresse (oder den Hostnamen) des Proxy-Servers und die entsprechende Port-Nummer angeben, die der Proxy-Server für Internetverbindungen verwendet.

    Wenn Sie diese Option nicht auswählen, wird der Download-Server eine Verbindung direkt zum CA-Server herstellen, (nicht über einen Proxy-Server).

Außerdem können Sie angeben, ob der Proxy-Server Authentifizierung benötigt. Wenn diese Option aktiviert ist, müssen zur Verwendung des Proxy-Servers Authentifizierungsinformationen (Benutzer-ID und Kennwort) angegeben werden.

- **Verbindung testen**: Mit dieser Option können Sie folgende Verbindungen testen und bei Abschluss eine Statusmeldung anzeigen:
  - Wenn Sie "CA Technologies-Server" als Download-Server ausgewählt haben, wird die Verbindung zwischen dem Computer und dem CA Technologies-Server über den angegebenen Proxy-Server getestet.
  - Wenn Sie "Staging-Server" als Download-Server angegeben haben, wird die Verbindung zwischen dem Computer und dem angegebenen Staging-Server getestet.

    Die Schaltfläche "Verbindung testen" wird verwendet, um die Verfügbarkeit der einzelnen aufgelisteten Staging-Server zu testen. Ein entsprechender Status wird im Feld "Verbindungsstatus" angezeigt.

  Hinweis: Die Testverbindung wird automatisch ausgeführt, wenn Sie beim Erstellen einer neuen Richtlinie das Dialogfeld der Voreinstellungen für automatische Aktualisierungen starten.

- **Ablaufplan für Aktualisierung**: Gibt an, wann auf neue CA ARCserve D2D-Aktualisierungen überprüft werden soll (die anschließend heruntergeladen werden sollen).

  Wenn diese Option ausgewählt wird, wird automatisch auf neue und verfügbare CA ARCserve D2D-Aktualisierungen geprüft. Wenn Sie diese Option auswählen, können Sie über ein Drop-down-Menü angeben, an welchen Tagen (täglich oder wöchentlich an einem bestimmten Tag) und zu welcher Uhrzeit diese Funktion ausgeführt werden soll.

  Wenn Sie diese Option auswählen und keinen Tag und keine Uhrzeit angeben, wird im Rahmen des Standardablaufplans jeden Sonntag um 4 Uhr eine automatische Überprüfung durchgeführt.

  Wenn diese Überprüfung feststellt, dass eine neue Aktualisierung verfügbar ist, wird CA ARCserve D2D die Aktualisierung automatisch herunterladen. Wenn Sie die Aktualisierungen nicht automatisch herunterladen möchten, können Sie diese Funktion in der Datei "D2DPMSettings.INI" deaktivieren. Weitere Informationen finden Sie im CA ARCserve D2D-Benutzerhandbuch auf der CA Support https://support.ca.com/cadocs/0/CA%20ARCserve%20D2D%20r16-ENU/Bookshelf.html-Website.

Wenn Sie diese Option nicht auswählen, werden alle automatischen Überprüfungen und Download-Funktionen deaktiviert (und der Status wird im Abschnitt der Statuszusammenfassung der Startseite angezeigt).

Diese Aktualisierungsfunktionen können nur manuell ausgelöst werden.

Hinweis: Wenn die Option konfiguriert wurde, erhalten Sie eine E-Mail-Benachrichtigung, wenn die geplante Überprüfung auf Aktualisierungen erkennt, dass eine neue Aktualisierung verfügbar ist.
E-Mail-Benachrichtigungen werden auch gesendet, wenn ein Fehler während der Überprüfung auf Aktualisierungen oder des Downloads auftritt.

5. Klicken Sie auf "Speichern".

Die Voreinstellungen der Aktualisierung werden gespeichert.

Bearbeiten oder Kopieren von Richtlinien

Mit CA ARCserve Central Protection Manager können Sie Richtlinien bearbeiten oder kopieren, nachdem sie erstellt wurden.

So bearbeiten Sie Richtlinien

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Richtlinien", um die Ansicht "Richtlinien" zu öffnen.

2. Klicken Sie im Fenster "Richtlinien" auf das Kontrollkästchen neben einer Richtlinie und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie in der Symbolleiste auf "Bearbeiten" und bearbeiten Sie die ausgewählte Richtlinie.
   - Klicken Sie in der Symbolleiste auf "Kopieren", um eine Richtlinie der ausgewählten Richtlinie zu kopieren und neu zu erstellen.

     Hinweis: Wenn Sie eine Richtlinie kopieren, öffnet sich das Dialogfeld "Richtlinie kopieren". Geben Sie einen Namen für die neue Richtlinie ein, und klicken Sie auf "OK".

   Das Dialogfeld "Richtlinie bearbeiten" wird geöffnet.

3. Wenn Sie den Namen der Richtlinie ändern wollen, geben Sie einen Namen im Feld "Richtliniennamen" an.

4. Geben Sie die benötigten Werte an und klicken Sie auf "Speichern".

Die Richtlinie wurde bearbeitet oder kopiert.

Löschen von Richtlinien

Mit CA ARCserve Central Protection Manager können Sie Richtlinien löschen, die zuvor erstellt wurden.

Hinweis: Mit CA ARCserve Central Protection Manager können Sie keine Richtlinien löschen, die Knoten zugewiesen sind. Um Richtlinien mit zugewiesenen Knoten zu löschen, müssen Sie die Zuweisung der Knoten zur Richtlinie aufheben und anschließend die Richtlinie löschen. Weitere Informationen darüber, wie Zuweisungen der Knoten zur Richtlinie aufgehoben werden, finden Sie unter Zuweisen und Aufheben der Zuweisung von Knoten aus Richtlinien (siehe Seite 140).

So löschen Sie Richtlinien

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

   Der Richtlinienbildschirm wird angezeigt.

2. Klicken Sie in der Liste "Richtlinien" auf die Richtlinie, die Sie löschen möchten.

3. Klicken Sie in der Symbolleiste "Richtlinien" auf "Löschen".

   Eine Bestätigungsmeldung des Löschvorgangs wird angezeigt.

4. Klicken Sie auf "Ja", um die Richtlinie zu löschen.

   Hinweis: Wenn Sie eine Richtlinie versehentlich löschen, müssen Sie die Richtlinie erneut erstellen. Wenn Sie die Richtlinie nicht löschen möchten, klicken Sie auf "Nein".

Die Richtlinie wird gelöscht.

Bereitstellen von Richtlinien

Mit CA ARCserve Central Protection Manager können Sie Richtlinien bereitstellen, falls das Programm mehrmals bereitgestellt wurde oder bei der Bereitstellung auf Remote-Server fehlschlug.

So stellen Sie Richtlinien bereit

1. Klicken Sie auf der CA ARCserve Central Protection Manager-Startseite in der Navigationsleiste auf "Richtlinien".

   Der Richtlinienbildschirm wird angezeigt.

2. Wählen Sie eine Richtlinie aus der Liste der Richtlinien aus und klicken Sie auf "Jetzt bereitstellen".

   Die Richtlinie wird unmittelbar bereitgestellt.

Hinweis: Wenn die Richtlinie erfolgreich für einen CA ARCserve D2D-Knoten bereitgestellt wurde, können die Einstellungen des CA ARCserve D2D-Knotens nicht geändert werden. Mit Ausnahme der aktivierten Schaltfläche "Verbindung aktualisieren" kann CA ARCserve D2D die Verbindungsinformationen am Sicherungsziel neu synchronisieren, wenn die Anmeldedaten auf dem Remote-Server geändert wurden. Außerdem können Sie den Richtlinienbereitstellungsstatus im Knotenlistenfenster in der Richtlinien-Spalte anzeigen.

Zuweisen und Aufheben der Zuweisung von Knoten aus Richtlinien

Mit CA ARCserve Central Protection Manager können Sie Knoten aus bestehenden D2D-Richtlinien zuweisen oder deren Zuweisung aufheben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite von CA ARCserve Central Protection Manager in der Navigationsleiste auf "Richtlinien", um das Fenster "Richtlinien" zu öffnen.
2. Wählen Sie eine Richtlinie aus der Liste der Richtlinien aus und klicken Sie auf die Registerkarte "Richtlinienzuweisung".

   Eine Liste von Knoten, die der ausgewählten Richtlinie zugewiesen sind, wird mit einem der folgenden Bereitstellungsaktionen und Status angezeigt (Format: *[Aktion] Bereitstellungsstatus*):

   - [Zuweisen] Ausstehend
   - [Zuweisung aufheben] Wird bereitgestellt
   - [Erneut synchronisieren] Fertig
   - [Aktualisierung] Fehlgeschlagen
   - [Erneut bereitstellen] D2D-Bereitstellung erfolgreich
   - [Erneut bereitstellen] D2D-Bereitstellung fehlgeschlagen
   - [Erneut bereitstellen] D2D-Bereitstellung wird neu gestartet
3. Klicken Sie auf die Schaltfläche "Zuweisen und Zuweisung aufheben".

   Das Dialogfeld "Zuweisung der Richtlinie durchführen/aufheben" wird geöffnet.
4. Geben Sie folgende Felder im Dialogfeld "Zuweisung der Richtlinie durchführen/aufheben" an:

   - **Gruppe:** Ermöglicht es Ihnen, den Gruppennamen auszuwählen, der die Knoten enthält, die Sie zuweisen möchten.
   - **Knotennamenfilter:** Lässt Sie die verfügbaren Knoten basierend auf einer Gemeinsamkeit filtern.

     Hinweis: Das Feld "Knotenname" ermöglicht es Ihnen, Knoten mithilfe von Platzhalterzeichen zu filtern.

     Acc* lässt Sie beispielsweise alle Knoten filtern, die einen Knotennamen haben, der mit "Acc." beginnt. Um die Filterergebnisse zu löschen, klicken Sie im Feld "Filter" auf X.

5. Führen Sie eine der folgenden Aktionen aus:

   - **Zuweisen von Knoten zu Richtlinien:** Wählen Sie die Knoten aus, die Sie hinzufügen möchten, und klicken Sie auf den einzelnen Rechtspfeil.

     Die Knoten werden von der Liste "Verfügbare Knoten" in die Liste "Ausgewählte Knoten" verschoben.

     Hinweis: Um alle Knoten auszuwählen und zu verschieben, klicken Sie auf den doppelten Rechtspfeil.

   - **Zuweisung der Knoten zu den Richtlinien aufzuheben:** Wählen Sie die Knoten aus, deren Zuweisung Sie aufheben möchten, und klicken Sie auf den einzelnen Rechtspfeil.

     Die Knoten bewegen sich von der Liste "Ausgewählte Knoten" zur Liste "Verfügbare Knoten".

     Hinweis: Um alle Knoten auszuwählen und zu verschieben, klicken Sie auf den doppelten Linkspfeil.

   Klicken Sie auf "OK".

   Hinweis: Die folgende Meldung wird angezeigt, wenn Sie die Zuweisung von Richtlinien aufheben:

   `Sie heben die Zuweisung der Richtlinien vom ausgewählten Knoten auf. Sie können die aktuellen Einstellungen beibehalten, damit der Knoten den Sicherungsvorgang fortsetzen kann. "Möchten Sie die Einstellungen beibehalten?" Klicken Sie auf "Ja", um die aktuellen CA ARCserve D2D-Einstellungen beizubehalten, auf "Nein", um die aktuellen CA ARCserve D2D-Einstellungen zu entfernen, oder auf "Abbrechen", um zum Bildschirm "Zuweisung der Richtlinie durchführen/aufheben" zurückzukehren.`

   Wenn Sie auf "Nein" klicken, gehen die CA ARCserve D2D-Remote-Einstellungen verloren und der CA ARCserve D2D-Server wird nicht geschützt.

Die Knoten werden auf die angegebenen Richtlinien angewendet.

Sicherung jetzt ausführen

Normalerweise werden Ihre Sicherungen automatisch durchgeführt und von den Ablaufplan-Einstellungen gesteuert. Es können jedoch auch sofortige Ad-Hoc-Sicherungen (vollständige Sicherungen, Zuwachssicherungen oder Überprüfungssicherungen) erforderlich sein.

Eine Ad-Hoc-Sicherung wird eher nach Bedarf und nicht im Voraus als Teil eines Sicherungsplans geplant. Wenn Sie z. B. größere Veränderungen an Ihrem Rechner durchführen möchten, kann es sein, dass Sie sofort eine Ad-Hoc-Sicherung durchführen möchten, ohne abzuwarten, bis die geplanten Wiederholungsintervalle für vollständige Sicherungen, Zuwachssicherungen oder Überprüfungssicherungen abgelaufen sind.

Mit einer Ad-hoc-Sicherung können Sie einen benutzerdefinierten (ungeplanten) Wiederherstellungspunkt hinzuzufügen, sodass Sie bei Bedarf auf den Stand zu diesem Zeitpunkt zurückgreifen können. Wenn Sie z. B. einen Patch oder ein Service Pack installiert haben, das sich negativ auf die Leistung Ihres Rechners auswirkt, haben Sie die Möglichkeit, das System auf den Stand der Ad-Hoc-Sicherung vor dieser Installation zurückzusetzen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.
2. Klicken Sie in der Navigationsleiste der Startseite auf "Knoten", um die Ansicht "Knoten" zu öffnen.
3. Führen Sie eine der folgenden Aktionen aus, um die Knoten festzulegen, die Sie sichern wollen:
   - **Knotenebene:** Klicken Sie auf die Gruppe, die die Knoten enthält, die Sie sichern wollen, und aktivieren Sie die Kontrollkästchen neben den Knoten, die Sie sichern wollen.
   - **Gruppenebene:** Klicken Sie auf die Gruppe, die die Knoten enthält, die Sie sichern wollen.
4. Führen Sie eine der folgenden Aktionen aus, um den Knoten zu sichern:
   - Klicken Sie in der Symbolleiste auf "Sichern".
   - Klicken Sie mit der rechten Maustaste auf die ausgewählte Gruppe oder klicken Sie mit der rechten Maustaste auf die Knoten und klicken Sie im Kontextmenü auf "Jetzt sichern".
5. Legen Sie im Dialogfeld "Sicherung jetzt ausführen" einen Sicherungstyp fest, indem Sie auf einen der folgenden Typen klicken:
   - **Vollständige Sicherung:** Startet eine vollständige Sicherung Ihres gesamten Rechners oder des ausgewählten Volumes.
   - **Zuwachssicherung:** Startet eine Zuwachssicherung Ihres Rechners. Eine Zuwachssicherung sichert nur jene Blöcke, die seit der letzten Sicherung geändert wurden.

     Hinweis: Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.

- **Überprüfungssicherung:** Startet eine Überprüfungssicherung Ihres Rechners, indem die aktuellste Sicherung von jedem einzelnen Block überprüft und der Inhalt und die Informationen mit der ursprünglichen Quelle verglichen wird. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht, aktualisiert CA ARCserve D2D die Sicherung dieses Blocks (Neusynchronisierung). Vergewissern Sie sich,dass Sie sich über die folgenden Vor- und Nachteile von Überprüfungssicherungen im Klaren sind:
  - Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein sehr kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.
  - Nachteile: Die Sicherung benötigt viel Zeit, da alle Blöcke des Quelldatenträgers mit den Blöcken der letzten Sicherung verglichen werden.

  Hinweis: Wenn Sie der Sicherungsquelle ein neues Volume hinzufügen, wird das neue Volume vollständig gesichert, unabhängig davon, welche allgemeine Sicherungsmethode ausgewählt wurde.

6. (Optional) Geben Sie einen Sicherungsnamen ein, und klicken Sie auf "OK". Wenn Sie keinen Namen angeben, wird die Sicherung standardmäßig Benutzerdefinierte/Vollständige/Zuwachs-/Überprüfungssicherung genannt.

Ein Bildschirm wird zur Bestätigung angezeigt, und der ausgewählte Sicherungstyp wird sofort gestartet.

Beachten Sie Folgendes:

- Alle in den Dialogfeldern der Richtlinien festgelegten Werte werden auf den Job angewendet.
- Wenn ein benutzerdefinierter Sicherungsjob (Ad-hoc) fehlschlägt, wird kein Ergänzungsjob erstellt. Ein Ergänzungsjob wird nur für geplante Jobs erstellt, die fehlschlagen.

Anzeigen von Jobstatusinformationen

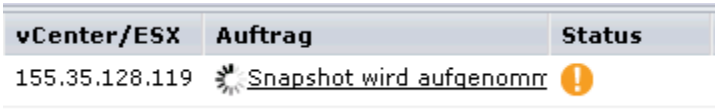
Wenn ein Job ausgeführt wird, können Sie detaillierte Informationen über den Job anzeigen. Optional können Sie einen sich in Bearbeitung befindenden Job anhalten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.
2. Klicken Sie in der Navigationsleiste der Startseite auf "Knoten", um die Ansicht "Knoten" zu öffnen.

3. Klicken Sie in der Baumstruktur "Gruppe" auf die Gruppe, die den Knoten enthält, für den Sie den Status des Jobs anzeigen wollen.

   Wenn der Job in Bearbeitung ist, wird die Phase des Jobs in der Spalte "Job" angezeigt.



4. Klicken Sie auf die Phase in der Spalte "Job", um das Dialogfeld "Statusüberwachung der Sicherung" zu öffnen.
5. Über das Dialogfeld "Statusüberwachung der Sicherung" können Sie einen der folgenden Schritte ausführen:
   - Klicken Sie auf "Schließen", um das Dialogfeld "Statusüberwachung der Sicherung" zu schließen.
   - Klicken Sie auf "Abbrechen", um den aktuellen Job anzuhalten.

     Hinweis: Das Dialogfeld "Statusüberwachung der Sicherung" schließt sich kurz nachdem Sie auf "Abbrechen" geklickt haben.

Wiederherstellen von Knoten in CA ARCserve Central Protection Manager

CA ARCserve Central Protection Manager stellt verschiedene Tools und Optionen bereit, mit denen Sie Knoten wiederherstellen können. In diesem Kapitel erfahren Sie, wie Sie Daten sicher und effektiv wiederherstellen können.

In diesem Abschnitt werden die folgenden Themen behandelt:

Wiederherstellen von Daten aus Wiederherstellungspunkten (siehe Seite 145)
Wiederherstellen von Daten aus Dateikopien (siehe Seite 148)
Wiederherstellen von Daten aus Dateien und Ordnern (siehe Seite 152)
Wiederherstellen von Daten von virtuellen Rechnern (siehe Seite 155)
Wiederherstellen von Microsoft Exchange-E-Mail-Daten (siehe Seite 160)

Wiederherstellen von Daten aus Wiederherstellungspunkten

Im Fenster "Wiederherstellungspunkte durchsuchen" können Sie Anwendungen wiederherstellen, indem Sie verfügbare Wiederherstellungspunkte (erfolgreiche Sicherungen) in einer Kalenderansicht durchsuchen.

So stellen Sie Daten aus Wiederherstellungspunkten wieder her

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".
2. Blenden Sie über die Ansicht "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen wollen.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen wollen, und danach in der Symbolleiste auf "Wiederherstellen".
3. Klicken Sie im Dialogfeld "Wiederherstellen" auf "Wiederherstellungspunkte durchsuchen".

   Das Dialogfeld "Wiederherstellungspunkte durchsuchen" wird angezeigt.
4. Geben Sie den Sicherungsspeicherort an oder durchsuchen Sie den Speicherort, an dem Ihre Sicherungs-Images gespeichert sind.

   Hinweis: Sie können auf den grünen Pfeil neben der Schaltfläche "Durchsuchen" klicken, um die Verbindung zum angegebenen Sicherungsziel zu überprüfen. Sie müssen möglicherweise die Anmeldeinformationen (Benutzername und Kennwort) eingeben, um mit einer Remote-Netzwerkfreigabe Verbindung aufzunehmen.

   Im Kalender sind alle Daten der angezeigten Zeitspanne, die Wiederherstellungspunkte für diese Sicherungsquelle enthalten, grün hervorgehoben.
5. Geben Sie an, welche Informationen wiederhergestellt werden sollen.
   a. Geben Sie das Datum für das Sicherungs-Image an, das Sie wiederherstellen möchten.

      Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit der Sicherung, Sicherungstyp, Name der Sicherung und Katalogstatus angezeigt.
   b. Wählen Sie einen Wiederherstellungspunkt aus, den Sie wiederherstellen möchten.

      Die entsprechenden Sicherungsinhalte (einschließlich Anwendungen) für diesen Wiederherstellungspunkt werden angezeigt.

c. Wählen Sie die Inhalte aus, die wiederhergestellt werden sollen.

- Bei einer Wiederherstellung auf Volume-Ebene können Sie angeben, ob das gesamte Volume oder ausgewählte Dateien bzw. Ordner wiederhergestellt werden sollen.
- Bei einer Wiederherstellung auf Anwendungsebene können Sie festlegen, ob die gesamte Anwendung, oder ausgewählte Komponenten, Datenbanken, Instanzen etc. wiederhergestellt werden sollen.

Klicken Sie auf "Weiter".

Das Dialogfeld "Optionen wiederherstellen" wird geöffnet.

6. Wählen Sie das Ziel für die Wiederherstellung aus.

Die verfügbaren Optionen können am ursprünglichen Speicherort der Sicherung, oder an einem anderen Speicherort wiederhergestellt werden.

Am ursprünglichen Speicherort wiederherstellen

Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

Hinweis: Wenn CA ARCserve D2D-Protokollordner auf dem ursprünglichen Speicherort wiederhergestellt werden, werden die Dateien, die sich in diesem Ordner befinden, übersprungen. Für CA ARCserve Central Host-Based VM Backup ist diese Option standardmäßig deaktiviert. Um sie zu verwenden, installieren Sie CA ARCserve D2D im Gast-Betriebssystem und führen Sie dann eine Wiederherstellung aus.

Wiederherstellen auf:

Sie können einen Speicherort für die Wiederherstellung der gesicherten Images angeben oder das System danach durchsuchen. Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen.

Wenn erforderlich, müssen Sie Benutzername und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.

7. Wählen Sie die Option zur Lösung durch CA ARCserve D2D von Konflikten aus, die während der Wiederherstellung erkannt werden.

   Es sind folgende Optionen verfügbar:

   Vorhandene Dateien überschreiben

   Überschreibt (ersetzt) alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind. Alle Objekte werden wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.

   Aktive Dateien ersetzen

   Ersetzt alle aktiven Dateien nach einem Neustart. Wenn CA ARCserve D2D während eines Wiederherstellungsversuchs erkennt, dass die vorhandene Datei gerade verwendet wird oder gerade auf sie zugegriffen wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

   Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien bei der Wiederherstellung übersprungen.

   Dateien umbenennen

   Erstellt eine neue Datei, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit dem gleichen Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten sind dann in einer neuen Datei wiederhergestellt.

   Vorhandene Dateien überspringen

   Überspringt alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, und überschreibt (ersetzt) sie nicht. Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

   Standardmäßig ist diese Option aktiviert.

8. (Optional) Wählen Sie "Stammverzeichnis erstellen" aus der Verzeichnisstruktur.

   Dies ermöglicht es CA ARCserve D2D, die gleiche Stammverzeichnisstruktur im Wiederherstellungspfad zu erstellen.

   Hinweis: Wenn diese Option nicht ausgewählt wird, wird die wiederherzustellende Datei oder der wiederherzustellende Ordner direkt im Zielordner wiederhergestellt.

9. Geben Sie das Verschlüsselungskennwort der Sicherung ein, um die verschlüsselten Daten wiederherzustellen. Klicken Sie anschließend auf "Weiter".

   Das Dialogfeld "Wiederherstellungs-Übersicht" wird angezeigt.

10. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.
    - Wenn die Zusammenfassung nicht korrekt ist, klicken Sie auf "Vorherige" und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.

Wenn die zusammenfassenden Informationen korrekt sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsprozess zu starten.

Wiederherstellen von Daten aus Dateikopien

Mit der Option "Nach Dateikopien suchen" können Sie Daten aus CA ARCserve D2D-Dateikopien wiederherstellen. Dateikopien sind Kopien von CA ARCserve D2D-Wiederherstellungspunkten, die Sie zur Offline-Speicherung beispielsweise auf Festplatten oder in die Cloud kopieren. Aus den Dateikopien können Sie die Daten festlegen, die Sie wiederherstellen wollen.

So stellen Sie Daten aus Dateikopien wieder her

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".
2. Blenden Sie über die Ansicht "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen wollen.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen wollen, und danach in der Symbolleiste auf "Wiederherstellen".
3. Klicken Sie im Dialogfeld "Wiederherstellen" auf "Nach Dateikopien suchen".

   Das Dialogfeld "Nach Dateikopien suchen" wird geöffnet.
4. Geben Sie vom Bereich "Namen" aus die Daten der Dateikopie an, die Sie wiederherstellen wollen. Sie können eine beliebige Kombination aus Dateien und Ordnern oder dem Volume festlegen.

   Wenn Sie eine individuelle Datei zur Wiederherstellung auswählen, werden alle kopierten Versionen dieser Datei im rechten Bereich angezeigt. Wenn mehrere Versionen verfügbar sind, wählen Sie die Version der Dateikopie aus, die Sie wiederherstellen wollen.

   - **Änderung:** Lässt Sie einen alternativen Speicherort suchen, an dem Ihre Dateikopie-Images gespeichert werden.

     Ein Dialogfeld wird geöffnet und zeigt verfügbare alternative Zieloptionen an:

     - **Lokaler oder Netzwerk-Treiber**: Das Dialogfeld "Speicherort für die Sicherung auswählen" wird geöffnet. Sie können einen alternativen Speicherort für Ihr lokales oder Netzwerklaufwerk suchen und auswählen.
     - **Cloud**: Das Dialogfeld "Cloud-Konfiguration" wird geöffnet und ermöglicht es Ihnen, auf einen alternativen Cloud-Speicherort zuzugreifen und ihn auszuwählen.

5. Klicken Sie auf "Weiter".

   Das Dialogfeld "Wiederherstellungsoptionen" wird geöffnet.

6. Füllen Sie im Dialogfeld "Wiederherstellungsoptionen" folgende Optionen aus:

   - **Ziel:** Wählen Sie das Ziel für die Wiederherstellung aus.
     - Am ursprünglichen Speicherort wiederherstellen: Ermöglicht es Ihnen, Dateien am ursprünglichen Speicherort wiederherzustellen, an dem das Sicherungs-Image erfasst wurde.
     - Wiederherstellen auf: Sie können einen Speicherort für die Wiederherstellung Ihrer Sicherungs-Images festlegen oder danach suchen. Klicken Sie auf den Pfeil neben dem Feld "Wiederherstellen auf", um die Verbindung zum angegebenen Speicherort zu überprüfen.

       Wenn erforderlich, müssen Sie Benutzername und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.
   - **Konfliktlösung:** Lässt Sie festlegen, wie CA ARCserve D2D Konflikte lösen soll, die während der Wiederherstellung festgestellt werden.
     - Vorhandene Dateien überschreiben: Lässt Sie vorhandene Dateien überschreiben (ersetzen), die am Wiederherstellungsziel gefunden werden. Alle Objekte werden wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.
     - Aktive Dateien ersetzen: Ermöglicht es Ihnen, aktive Dateien nach Neustart zu ersetzen. Wenn CA ARCserve D2D während eines Wiederherstellungsversuchs entdeckt, dass die vorhandene Datei gerade verwendet wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

       Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien im Wiederherstellungsprozess übersprungen.
     - Dateien umbenennen: Lässt Sie neue Dateien erstellen, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit dem gleichen Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten werden dann in einer neuen Datei wiederhergestellt.
     - Vorhandene Dateien überspringen: Lässt Sie alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, überspringen und nicht überschreiben (ersetzen). Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

       Standardmäßig ist diese Option aktiviert.

- **Verzeichnisstruktur:** Lässt Sie festlegen, was CA ARCserve D2D während der Wiederherstellung mit der Verzeichnisstruktur vornehmen wird oder nicht.
  - Stammverzeichnis erstellen: Lässt Sie festlegen, dass, falls eine Verzeichnisstruktur im erfassten Sicherungs-Image vorhanden ist, CA ARCserve D2D die gleiche Verzeichnisstruktur am Wiederherstellungszielpfad erstellt.

    Wenn die Option "Stammverzeichnis erstellen" nicht ausgewählt (deaktiviert) ist, werden die ausgewählten Dateien/Ordner direkt im Zielordner wiederhergestellt.

    Beispiel:

    Sie haben während der Sicherung die Dateien "C:\Ordner1\Unterordner2\A.txt" und "C:\Ordner1\Unterordner2\B.txt" erfasst und als Wiederherstellungsziel "D:\Wiederherstellen" ausgewählt.

    Wenn Sie die Wiederherstellung der Dateien "A.txt" und "B.txt" einzeln festgelegt haben, werden die Dateien in "D:\Wiederherstellen\A.txt" und "D:\Wiederherstellen\B.txt" wiederhergestellt (das Stammverzeichnis über der ausgewählten Dateiebene wird nicht wiederhergestellt).

    Wenn Sie eine Wiederherstellung auf "Unterordner2"-Ebene auswählen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Unterordner2\A.txt" und "D:\Wiederherstellen\Unterordner2\B.txt" (das Stammverzeichnis über der ausgewählten Ordnerebene wird nicht wiederhergestellt).

    Wenn die Option "Stammverzeichnis erstellen" ausgewählt (aktiviert) ist, wird der gesamte Stammverzeichnispfad für die Dateien/Ordner (einschließlich Volume-Name) im Zielordner wiederhergestellt. Wenn Dateien/Ordner vom selben Volume-Name wiederhergestellt werden sollen, ist dieser Volume-Name nicht im Wiederherstellungsziel-Stammverzeichnispfad enthalten. Wenn Dateien/Ordner von einem anderen Volume-Name wiederhergestellt werden sollen, enthält der Wiederherstellungsziel-Stammverzeichnispfad diesen Volume-Namen.

    Beispiel:

    Sie haben während der Sicherung die Dateien"C:\Ordner1\Unterordner2\A.txt", "C:\Ordner1\Unterordner2\B.txt" und E:\Ordner3\Unterordner4\C.txt erfasst, und bei der Wiederherstellung "D:\Wiederherstellen" als Wiederherstellungsziel ausgewählt.

    Wenn Sie nur die Datei "A.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\Ordner1\Unterordner2\A.txt" (das gesamte Stammverzeichnis wird ohne den Volume-Namen erneut erstellt).

Wenn Sie die Dateien "A.txt" und "C.txt" wiederherstellen, ist das Wiederherstellungsziel "D:\Wiederherstellen\C\Ordner1\Unterordner2\A.txt" und "D:\Wiederherstellen\ E\Ordner3\Unterordner4\C.txt" (das gesamte Stammverzeichnis wird mit dem Volume-Namen erneut erstellt).

- **Verschlüsselungskennwort:** Wenn die Wiederherstellungspunktdaten, die Sie versuchen wiederherzustellen, verschlüsselt sind, müssen Sie möglicherweise das Verschlüsselungskennwort angeben.

  Ein Kennwort ist nicht erforderlich, wenn Sie versuchen, die Wiederherstellung auf dem gleichen Rechner durchzuführen, auf dem die verschlüsselte Sicherung ausgeführt wurde. Wenn Sie jedoch versuchen, die Wiederherstellung auf einem anderen Rechner durchzuführen, ist ein Kennwort erforderlich.

  Hinweis: Die folgenden Symbole zeigen an, ob der Wiederherstellungspunkt verschlüsselte Informationen enthält, und können ein Kennwort zur Wiederherstellung benötigen.

  Nicht verschlüsselter Wiederherstellungspunkt (Uhrsymbol):

  Verschlüsselter Wiederherstellungspunkt (Uhr mit Sperrsymbol):

Klicken Sie auf "Weiter".

Das Dialogfeld "Wiederherstellungs-Übersicht" wird geöffnet.

7. Überprüfen Sie, ob die Informationen auf dem Dialogfeld "Wiederherstellungs-Übersicht" richtig sind.

   Hinweis: Wenn Sie die Wiederherstellungsoptionen, die Sie festgelegt haben, ändern wollen, klicken Sie auf "Zurück" und gehen Sie zum zutreffenden Dialogfeld, um die Werte zu ändern.

   Klicken Sie auf Fertig stellen.

Die Wiederherstellungsoptionen werden angewendet und die Daten werden wieder hergestellt.

Wiederherstellen von Daten aus Dateien und Ordnern

Bei jeder erfolgreichen Sicherung durch die Anwendung werden alle gesicherten Dateien oder Ordner zum Snapshot-Image der Sicherung hinzugefügt. Mit dieser Wiederherstellungsmethode können Sie genau festlegen, welche Dateien oder Ordner wiederhergestellt werden sollen.

So stellen Sie Daten aus Dateien und Ordnern wieder her

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Blenden Sie über die Ansicht "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen wollen.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen wollen, und danach in der Symbolleiste auf "Wiederherstellen".

2. Klicken Sie im Dialogfeld "Wiederherstellen" auf "Wiederherzustellende Dateien/Ordner suchen".

   Das Dialogfeld "Wiederzustellende Dateien/Ordner suchen" wird geöffnet.

3. Geben Sie den "Speicherort für die Sicherung" und den "Speicherort der Dateikopie" an oder durchsuchen Sie den Speicherort, an dem die Sicherungs-Images gespeichert sind.

   Beachten Sie Folgendes:

   - Für "Speicherort für die Sicherung" können Sie auf den grünen Pfeil neben der Schaltfläche "Durchsuchen" klicken, um die Verbindung zum angegebenen Sicherungsziel zu überprüfen. Sie müssen möglicherweise die Anmeldeinformationen (Benutzername und Kennwort) eingeben, um mit einer Remote-Netzwerkfreigabe Verbindung aufzunehmen.
   - Für "Speicherort der Dateikopie" können Sie auf die Schaltfläche "Änderung" klicken, um auf ein lokales Ziel, ein Netzwerklaufwerk oder eine Cloud zu wechseln. Weitere Details zum Speicherort der Dateikopie finden Sie unter Wiederherstellung von Dateikopien (siehe Seite 148).

4. Geben Sie den Namen der Datei oder des Ordners, der wiederhergestellt werden soll, an.

   Hinweis: Das Feld "Dateiname" unterstützt die Suche nach vollständigen Namen oder mit Platzhaltern. Wenn Ihnen der vollständige Dateiname nicht bekannt ist, können Sie die Abfrage vereinfachen, indem Sie die Platzhalter "*" und "?" im Feld "Dateiname" eingeben.

   Folgende Platzhalter für den Datei- oder Ordnernamen werden unterstützt:

   - "*": Verwenden Sie den Asterisk, um null oder mehr Zeichen in einem Datei- oder Ordnernamen zu ersetzen.
   - "?": Verwenden Sie das Fragezeichen, um ein einzelnes Zeichen in einem Datei- oder Ordnernamen zu ersetzen.

   Beispiel: Wenn Sie *.txt angeben, werden alle Dateien mit einer .txt-Dateierweiterung in den Suchergebnissen angezeigt.

5. (Optional) Geben Sie einen Pfadnamen an, um Ihre Suche noch weiter zu filtern und wählen Sie aus, ob Unterverzeichnisse, Dateien und Ordner in der Suche berücksichtigt werden.

6. Klicken Sie auf "Suchen", um die Suche zu starten.

   Die Suchergebnisse werden angezeigt. Wenn mehrere Wiederherstellungspunkte für dieselbe Datei gefunden werden, werden alle Wiederherstellungspunkte nach Datum geordnet aufgelistet (der aktuellste steht an erster Stelle).

7. Wählen Sie aus der Liste die wiederherzustellende Version aus, und klicken Sie auf "Weiter".

   Das Dialogfeld "Optionen wiederherstellen" wird geöffnet.

8. Wählen Sie das Ziel für die Wiederherstellung aus.

   Die verfügbaren Optionen können am ursprünglichen Speicherort der Sicherung, oder an einem anderen Speicherort wiederhergestellt werden.

   Am ursprünglichen Speicherort wiederherstellen

   Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

   Hinweis: Wenn CA ARCserve D2D-Protokollordner auf dem ursprünglichen Speicherort wiederhergestellt werden, werden die Dateien, die sich in diesem Ordner befinden, übersprungen.

   Wiederherstellen auf:

   Sie können einen Speicherort für die Wiederherstellung der gesicherten Images angeben oder das System danach durchsuchen. Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen.

   Wenn erforderlich, müssen Sie Benutzername und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.

9. Wählen Sie die Option zur Lösung durch CA ARCserve D2D von Konflikten aus, die während der Wiederherstellung erkannt werden.

   Es sind folgende Optionen verfügbar:

   Vorhandene Dateien überschreiben

   Überschreibt (ersetzt) alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind. Alle Objekte werden wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.

   Aktive Dateien ersetzen

   Ersetzt alle aktiven Dateien nach einem Neustart. Wenn CA ARCserve D2D während eines Wiederherstellungsversuchs erkennt, dass die vorhandene Datei gerade verwendet wird oder gerade auf sie zugegriffen wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

   Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien bei der Wiederherstellung übersprungen.

   Dateien umbenennen

   Erstellt eine neue Datei, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit dem gleichen Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten sind dann in einer neuen Datei wiederhergestellt.

   Vorhandene Dateien überspringen

   Überspringt alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind, und überschreibt (ersetzt) sie nicht. Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

   Standardmäßig ist diese Option aktiviert.

10. (Optional) Wählen Sie "Stammverzeichnis erstellen" aus der Verzeichnisstruktur.

    Dies ermöglicht es CA ARCserve D2D, die gleiche Stammverzeichnisstruktur im Wiederherstellungspfad zu erstellen.

    Hinweis: Wenn diese Option nicht ausgewählt wird, wird die wiederherzustellende Datei oder der wiederherzustellende Ordner direkt im Zielordner wiederhergestellt.

11. Geben Sie das Verschlüsselungskennwort der Sicherung ein, um die verschlüsselten Daten wiederherzustellen. Klicken Sie anschließend auf "Weiter".

    Das Dialogfeld "Wiederherstellungs-Übersicht" wird angezeigt.

12. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.

    - Wenn die Zusammenfassung nicht korrekt ist, klicken Sie auf "Vorherige" und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.

Wenn die zusammenfassenden Informationen korrekt sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsprozess zu starten.

Wiederherstellen von Daten von virtuellen Rechnern

Verwenden Sie die Option zur Wiederherstellung der VM, um einen virtuellen Rechner, den Sie zuvor gesichert haben, wiederherzustellen.

So stellen Sie Daten von virtuellen Rechnern wieder her

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Blenden Sie über die Ansicht "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen wollen.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen wollen, und danach in der Symbolleiste auf "Wiederherstellen".

2. Klicken Sie im Dialogfeld "Wiederherstellen" auf "VM wiederherstellen".

   Das Dialogfeld "Wiederherstellen" wird geöffnet.

3. Geben Sie den Speicherort für die Sicherung (Quelle) an. Sie können den Speicherort der Sicherungs-Images angeben oder das System danach durchsuchen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten. Klicken Sie auf das grüne Pfeilsymbol, um zu überprüfen, ob ein ordnungsgemäßer Zugriff auf den Speicherort der Sicherungsquelle besteht.

   Im Kalender sind alle Daten für die angezeigte Zeitspanne, die Wiederherstellungspunkte für diese Sicherungsquelle enthalten, grün hervorgehoben.

4. Geben Sie den wiederherzustellenden virtuellen Rechner an.

   Das Drop-down-Menü schließt alle virtuellen Rechner am angegebenen Speicherort für die Sicherung ein.

5. Geben Sie das Datum für das Image des virtuellen Rechners an, das Sie wiederherstellen möchten.

   Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp und Name der Sicherung angezeigt.

6. Wählen Sie einen Wiederherstellungspunkt aus, den Sie wiederherstellen möchten.

   Die entsprechenden Sicherungsinhalte (einschließlich Anwendungen) für diesen Wiederherstellungspunkt werden lediglich als Referenz angezeigt. Wenn Sie einen virtuellen Rechner wiederherstellen, wird der gesamte Rechner wiederhergestellt. Dadurch können Sie individuelle Volumes, Ordner oder Dateien innerhalb des ausgewählten virtuellen Rechners anzeigen, aber nicht auswählen.

   Hinweis: Eine Uhr mit einem Sperrsymbol zeigt an, dass der Wiederherstellungspunkt verschlüsselte Informationen enthält und möglicherweise ein Kennwort zur Wiederherstellung benötigt.

7. Geben Sie die gesicherten Informationen an, die wiederhergestellt werden sollen, und klicken Sie auf "Weiter".

   Das Dialogfeld "Optionen wiederherstellen" wird geöffnet.

8. Wählen Sie das Wiederherstellungsziel aus.

   Am ursprünglichen Speicherort wiederherstellen

   Stellt den virtuellen Rechner am selben Speicherort wieder her, an dem das Sicherungs-Image erstellt wurde. Standardmäßig ist diese Option aktiviert.

   Weitere Informationen finden Sie im Abschnitt Wiederherstellung der VM am ursprünglichen Speicherort.

   An einem alternativen Speicherort wiederherstellen

   Stellt den virtuellen Rechner an einem anderen Speicherort wieder her, an dem das Sicherungs-Image erstellt wurde.

   Weitere Informationen finden Sie im Abschnitt Wiederherstellung der VM an einem alternativen Speicherort.

9. Legen Sie fest, auf welche Weise CA ARCserve D2D Konflikte, die während der Wiederherstellung auftreten, lösen soll.

   Die verfügbare Option bestimmt, ob der vorhandene virtuelle Rechner überschrieben werden soll. Standardmäßig ist diese Option zum Überschreiben deaktiviert.

   - Wenn Sie diese Option auswählen, wird der Wiederherstellungsvorgang alle vorhandenen Images dieses virtuellen Rechners, die sich am angegebenen Wiederherstellungsziel befinden, überschreiben (bzw. ersetzen). Das Image des virtuellen Rechners wird von den Sicherungsdateien wiederhergestellt, unabhängig davon, ob sie derzeit auf Ihrem Wiederherstellungsziel vorhanden sind.
   - Wenn Sie diese Option nicht aktivieren, erstellt der Wiederherstellungsvorgang ein separates Image für diesen virtuellen Rechner und überschreibt am angegebenen Wiederherstellungsziel keine vorhandenen Images.

10. Legen Sie die Option "Nach der Wiederherstellung" fest.

    Wählen Sie, ob die Stromzufuhr für den virtuellen Rechner am Ende des Wiederherstellungsvorgangs angewendet werden soll. Standardmäßig ist diese Option für die Stromzufuhr deaktiviert.

Wiederherstellen von virtuellen Rechnern an ursprünglichen Speicherorten

Während des Konfigurationsvorgangs zur Wiederherstellung der VM ist es erforderlich, dass Sie die Option auswählen, mit der Sie bestimmen können, wo der virtuelle Rechner wiederhergestellt wird. Die verfügbare Auswahl ist "Wiederherstellung am ursprünglichen Speicherort" und "Wiederherstellung an einem alternativen Speicherort".

Wenn Sie Ihre VM am ursprünglichen Speicherort wiederherstellen, führen Sie folgende Schritte aus:

So stellen Sie virtuelle Rechner an ursprünglichen Speicherorten wieder her

1. Wählen Sie im Dialogfeld "Wiederherstellungsoptionen", nachdem Sie die Optionen "Konflikte lösen" und "Nach der Wiederherstellung" angegeben haben, die Option "Am ursprünglichen Speicherort wiederherstellen" und klicken Sie auf "Weiter".

   Hinweis: Weitere Informationen über die Optionen "Konflikte lösen" und "Nach der Wiederherstellung" finden Sie im Abschnitt Wiederherstellen von Daten aus virtuellen Rechnern (siehe Seite 155).

   Das Dialogfeld "Anmeldeinformationen für Quell-vCenter/ESX Server festlegen" wird angezeigt.

2. Geben Sie die Anmeldeinformationen ein, um auf den virtuellen Rechner zuzugreifen.

   - **vCenter/ESX Server**: Geben Sie den Hostnamen oder die IP-Adresse für das Ziel des vCenter- oder ESX-Serversystems an.
   - **VM Name:** Zeigt den Hostnamen des virtuellen Rechners an, den Sie wiederherstellen.
   - **Protokoll:** Geben Sie das Protokoll an, das Sie für die Kommunikation mit dem Zielserver verwenden möchten. Die verfügbare Auswahl ist "HTTP" und "HTTPS".
   - **Portnummer:** Legen Sie den Port fest, den Sie für die Kommunikation zwischen dem Quellserver und dem Ziel verwenden möchten. Standardmäßig wird die Portnummer 443 angegeben.
   - **Benutzername:** Legen Sie den Benutzernamen fest, der über Zugriffsrechte zur Anmeldung am virtuellen Rechner, den Sie wiederherstellen, verfügt.
   - **Kennwort:** Geben Sie das entsprechende Kennwort für den Benutzernamen an, der für die Anmeldung am virtuellen Rechner, der wiederhergestellt wird, erforderlich ist.

3. Wenn alle Anmeldeinformationen angegeben sind, klicken Sie auf "OK".

   Das Dialogfeld "Wiederherstellungs-Übersicht" wird geöffnet.

4. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.

   - Wenn die Zusammenfassung nicht korrekt ist, klicken Sie auf "Vorherige" und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
   - Wenn die zusammenfassenden Informationen korrekt sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsprozess zu starten.

Wiederherstellen von virtuellen Rechnern an alternativen Speicherorten

Während des Konfigurationsvorgangs zur Wiederherstellung der VM ist es erforderlich, dass Sie die Option auswählen, mit der Sie bestimmen können, wo der virtuelle Rechner wiederhergestellt wird. Die verfügbare Auswahl ist "Wiederherstellung am ursprünglichen Speicherort" und "Wiederherstellung an einem alternativen Speicherort".

Wenn Sie den virtuellen Rechner an einem alternativen Speicherort wiederherstellen wollen, führen Sie folgende Schritte aus:

So stellen Sie virtuelle Rechner an alternativen Speicherorten wieder her

1. Wählen Sie im Dialogfeld "Wiederherstellungsoptionen", nachdem Sie die Optionen "Konflikte lösen" und "Nach der Wiederherstellung" angegeben haben, die Option "An einem alternativen Speicherort wiederherstellen".

   Hinweis: Weitere Informationen über die Optionen "Konflikte lösen" und "Nach der Wiederherstellung" finden Sie im Abschnitt Wiederherstellen von Daten auf virtuellen Rechnern (siehe Seite 155).

   Das Dialogfeld "Wiederherstellungsoptionen" wird eingeblendet, um zusätzliche Optionen für Wiederherstellungen an alternativen Speicherorten anzuzeigen.

2. Geben Sie vCenter/ESX Server-Informationen an.
   - **vCenter/ESX Server**: Geben Sie den Hostnamen oder die IP-Adresse für das Ziel des vCenter- oder ESX-Serversystems an.
   - **Benutzername**: Legen Sie den Benutzernamen fest, der über Zugriffsrechte zur Anmeldung am virtuellen Rechner, den Sie wiederherstellen, verfügt.
   - **Kennwort:** Geben Sie das entsprechende Kennwort für den Benutzernamen an, der für die Anmeldung am virtuellen Rechner, der wiederhergestellt wird, erforderlich ist.
   - **Protokoll:** Geben Sie das Protokoll an, das Sie für die Kommunikation mit dem Zielserver verwenden möchten. Die verfügbare Auswahl ist "HTTP" und "HTTPS".
   - **Portnummer:** Legen Sie den Port fest, den Sie für die Kommunikation zwischen dem Quellserver und dem Ziel verwenden möchten. Standardmäßig wird die Portnummer 44 angegeben.
3. Wenn die vCenter/ESX Server-Informationen angegeben sind, klicken Sie auf die Schaltfläche "Stellen Sie eine Verbindung zum vCenter/ESX Server her".

   Wenn die alternativen Anmeldeinformationen für den Serverzugriff korrekt sind, werden die Felder "Weitere Informationen" aktiviert.
4. Geben Sie weitere Informationen an.
   - **VM Name:** Zeigt den Hostnamen des virtuellen Rechners an, den Sie wiederherstellen.
   - **ESX Server:** Legen Sie den Ziel-ESX-Server fest. Das Drop-down-Menü enthält eine Auflistung aller ESX-Server, die mit dem angegebenen virtuellen Rechner verbunden sind.
   - **VM DataStore**: Legen Sie das Ziel des VM-Datenspeichers fest.
5. Wenn "Weitere Informationen" angegeben sind, klicken Sie auf "Weiter".

   Das Dialogfeld "Wiederherstellungs-Übersicht" wird geöffnet.
6. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.
   - Wenn die Zusammenfassung nicht korrekt ist, klicken Sie auf "Vorherige" und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
   - Wenn die zusammenfassenden Informationen korrekt sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsprozess zu starten.

Wiederherstellen von Microsoft Exchange-E-Mail-Daten

Jedes Mal, wenn CA ARCserve D2D eine erfolgreiche Sicherung ausführt, wird gleichzeitig ein Snapshot-Image Ihrer Sicherung erstellt. Diese Sammlung an Wiederherstellungspunkten ermöglicht es Ihnen, das Sicherungs-Image, das Sie wiederherstellen möchten, zu finden und genau anzugeben. Für Microsoft Exchange Server können Sie dann diese Wiederherstellungspunkte durchsuchen, um die individuellen Objekte (Postfächer, Postfachordner oder Mail) zu lokalisieren, die Sie wiederherstellen möchten. Um eine spezifische Wiederherstellung von Exchange auszuführen, muss das Konto über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie im Abschnitt Erforderliche Berechtigungen für Exchange-Konten.

Hinweis: Für Microsoft Exchange Server 2007 und höher ist Messaging API (MAPI) eine Voraussetzung für die spezifische Wiederherstellung von Exchange-Objekten. Wenn MAPI nicht auf Ihrem Exchange Server, Postfach oder auf der Mailebene installiert ist, werden spezifische Wiederherstellungen möglicherweise fehlschlagen. Weitere Informationen über die Installation von MAPI auf Ihrem Exchange Server finden Sie im Microsoft Download Center.

So stellen Sie Microsoft Exchange-E-Mail-Daten wieder her

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Blenden Sie über die Ansicht "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen wollen.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen wollen, und danach in der Symbolleiste auf "Wiederherstellen".

2. Klicken Sie vom Dialogfeld "Wiederherstellen" auf "Exchange-E-Mails wiederherstellen".

   Das Dialogfeld "Exchange-E-Mails wiederherstellen" wird geöffnet.

3. Geben Sie den Speicherort für die Sicherung an. Sie können den Speicherort der Sicherungs-Images angeben oder das System danach durchsuchen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten. Klicken Sie auf das grüne Pfeilsymbol, um zu überprüfen, ob ein ordnungsgemäßer Zugriff auf den Speicherort der Sicherungsquelle besteht.

   Im Kalender sind alle Daten für die angezeigte Zeitspanne, die Wiederherstellungspunkte für diese Sicherungsquelle enthalten, grün hervorgehoben.

4. Geben Sie das Datum für das Sicherungs-Image an, das Sie wiederherstellen möchten.

   Es werden die entsprechenden Exchange-Postfachdatenbanken einschließlich Uhrzeit, Sicherungstyp und Name der Sicherung angezeigt.

5. Wählen Sie eine Exchange-Postfachdatenbank, die Sie wiederherstellen möchten, und klicken Sie auf "Weiter".

   Hinweis: Eine Benachrichtigung wird angezeigt, in der Sie gefragt werden, ob Sie zu diesem Zeitpunkt einen Katalog für die spezifische Wiederherstellung von Exchange-Objekten generieren wollen. Wenn Sie bei der Generierung des Katalogs "Nein" auswählen, werden Sie keine detaillierten Wiederherstellungspunkte durchsuchen oder auswählen können. Dadurch können Sie eine vollständige Datenbankwiederherstellung nur über das Dialogfeld "Wiederherstellungspunkte durchsuchen" durchführen.

   Das Dialogfeld "Wiederherstellungsoptionen" wird angezeigt und die entsprechende Liste des Postfachinhalts für die ausgewählte Datenbank wird aufgelistet.

   Hinweis: Nur E-Mail-Wiederherstellung wird unterstützt. Die Wiederherstellung von Kalendern, Kontakten, Hinweisen und Aufgabenelementen wird nicht unterstützt.

6. Wählen Sie die Ebene des bzw. der wiederherzustellenden Exchange-Objekts/-e aus (Postfach, Ordner oder individuelle Mail).

   Hinweis: Sie können den gesamten Inhalt, einen Teil des Inhalts oder mehrere Exchange-Objekte zur Wiederherstellung auswählen.

   a. Wenn Sie eine Postfachdatenbank auswählen, werden alle Postfächer in dieser Datenbank wiederhergestellt.

   b. Wenn Sie eine Postfachebene auswählen, wird der gesamte entsprechende Inhalt (Ordner und individuelle Mail) innerhalb des Postfachs wiederhergestellt.

   c. Wenn Sie die Postfachordnerebene auswählen, wird der gesamte entsprechende Mail-Inhalt innerhalb des Ordners wiederhergestellt.

   d. Wenn Sie die individuelle Mail-Ebene auswählen, werden nur die ausgewählten Mail-Objekte wiederhergestellt.

      Hinweis: Für Exchange 2003 gilt, wenn die wiederherzustellende Mail über einen anderen E-Mail-Client als Outlook gesendet wurde und die Mail bei der Sicherung über einen Kennzeichnungsstatus verfügt hat, wird die Mail selbst zwar wiederhergestellt, aber die beigefügte Markierung wird nicht mit eingeschlossen.

7. Klicken Sie auf "Weiter".
8. Wählen Sie das Ziel für die Wiederherstellung aus.

   Die verfügbaren Optionen können am ursprünglichen Speicherort der Sicherung, oder an einem anderen Speicherort wiederhergestellt werden.

   Hinweise:

   - Wenn ein Postfach oder eine Mail (am ursprünglichen oder an einem alternativen Speicherort) wiederhergestellt wird, sollten Sie sicherstellen, dass das Ziel verfügbar ist, da der Wiederherstellungsversuch sonst fehlschlagen wird. CA ARCserve D2D validiert das Ziel nur dann, wenn der Wiederherstellungsjob übergeben wird.
   - Wenn Sie versuchen, Mails auf einem Rechner wiederherzustellen, auf dem die E-Mail-Adressen in diesen Mails nicht zulässig sind (nicht in der Domäne vorhanden sind), oder wenn sich der Benutzer nicht im Postfach angemeldet hat, werden einige Felder nach der Sicherung möglicherweise nicht identisch angezeigt.
   - Für Exchange 2010 können archivierte Postfachelemente nicht am ursprünglichen Speicherort wiederhergestellt werden. Archivierte Postfachelemente können nur an einem alternativen Speicherort oder auf einem lokalen Datenträger wiederhergestellt werden. Außerdem können normale Postfachelemente nicht wiederhergestellt werden, um Postfächer zu archivieren.

   Am ursprünglichen Speicherort wiederherstellen

   Stellt die E-Mails am selben Speicherort wieder her, an dem das Sicherungs-Image erstellt wurde. Mails behalten die gleiche Hierarchie bei und werden am ursprünglichen Postfach und im ursprünglichen Ordner wiederhergestellt.

   - Wenn der derzeitige Rechner nicht der aktive Exchange-Server ist, wird CA ARCserve D2D den Speicherort des aktiven Servers erkennen und die Mails auf dem aktiven Server wiederherstellen.
   - Wenn das Postfach innerhalb derselben Organisation auf einen anderen Exchange-Server verschoben wurde, erkennt CA ARCserve D2D den neuen Exchange-Server, auf dem sich das ursprüngliche Postfach befindet und führt die Wiederherstellung auf dem neuen Server durch.
   - Wenn der Anzeigename des Postfachs geändert wurde, kann das Postfach (von einer früheren Sicherungssitzung) nicht am ursprünglichen Speicherort wiederhergestellt werden, da CA ARCserve D2D den geänderten Namen nicht finden kann. Um dieses Problem zu lösen, können Sie angeben, dass dieses Postfach an einem alternativen Speicherort wiederhergestellt werden soll.

Nur Speicherauszugsdatei

Stellt die E-Mails auf einem Datenträger wieder her. Dieser Speicherort muss ein lokaler Pfad sein. Die wiederhergestellten Mails werden die gleiche Hierarchie wie im entsprechenden Exchange-Postfach beibehalten. Der Dateiname wird der Betreff der E-Mail sein.

Hinweis: Wenn der E-Mail-Betreff, der Ordnername oder der Postfachname einen der folgenden Zeichen enthält, wird das Zeichen durch einen Bindestrich (-) im Dateinamen ersetzt: \ / : * ? " < > |

Es gibt zwei Optionen, um eine Konfliktsituation in einem Dateisystem zu lösen. Zwei Dateien im Dateisystem können nicht im gleichen Ordner vorhanden sein, während dies nicht für Exchange-Mails gilt.

- **Umbenennen:** Wenn auf dem Datenträger eine Datei vorhanden ist, die den gleichen Namen trägt, wie der E-Mail-Betreff, gibt CA ARCserve D2D den E-Mail-Betreff an und erweitert ihn am Ende um eine Zahl.
- **Überschreiben:**Falls es auf dem Datenträger eine Datei gibt, die den gleichen Namen hat wie der E-Mail-Betreff, überschreibt CA ARCserve D2D diese Datei.

An einem alternativen Speicherort wiederherstellen

Stellt die Mails an einem angegebenen Speicherort wieder her oder ermöglicht es Ihnen, den Speicherort zu durchsuchen, an dem Ihre Sicherungs-Images wiederhergestellt werden. Das Ziel muss ein Postfach in der gleichen Exchange-Organisation sein und ein neuer Ordnername ist erforderlich. (Wenn Sie versuchen, Mails an einem alternativen Speicherort wiederherzustellen, kann das Ziel kein öffentlicher Ordner sein)

Nachdem Sie den Benutzernamen und das Kennwort eingegeben haben, können Sie auf die Schaltfläche "Durchsuchen" klicken, um durch eine Liste aller Exchange-Server, Speichergruppen, Exchange-Datenbanken und Postfächer in der aktuellen Organisation zu navigieren.

Wählen Sie ein beliebiges Postfach als Ziel aus.

9. Klicken Sie auf "Weiter".

   Das Dialogfeld "Wiederherstellungs-Übersicht" wird angezeigt.

10. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.

    - Wenn die Zusammenfassung nicht korrekt ist, klicken Sie auf "Vorherige" und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
    - Wenn die zusammenfassenden Informationen korrekt sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsprozess zu starten.

    Hinweis: Wenn der Katalog- und Wiederherstellungsjob für die spezifische Wiederherstellung von Exchange-Objekten in Bearbeitung ist, befindet sich die Sicherungssitzung im geladenen Status. Führen Sie auf diesem geladenen Volume keine Vorgänge aus (Formatieren, Laufwerksbuchstaben ändern, Partitionen löschen usw.).

Anzeigen von CA ARCserve Central Protection Manager-Protokollen

Das Anzeigeprotokoll enthält umfassende Informationen zu den Vorgängen, die von Ihrer Anwendung ausgeführt werden. Das Protokoll liefert einen Audit-Pfad für jeden ausgeführten Job (an erster Stelle werden die letzten Aktivitäten aufgelistet) und kann bei der Behebung von Fehlern hilfreich sein.

So zeigen Sie CA ARCserve Central Protection Manager-Protokolle an

1. Klicken Sie auf der Startseite in der Navigationsleiste auf "Protokolle anzeigen".

   Das Fenster "Protokolle anzeigen" wird angezeigt.

2. Geben Sie in den Drop-down-Listen die Protokollinformationen an, die Sie anzeigen möchten.

   - **Schweregrad:** Lässt Sie den Schweregrad des Protokolls angeben, das Sie anzeigen möchten. Sie können folgende Schweregradoptionen angeben:
     - **Alle:** Zeigt alle Protokolle unabhängig vom Schweregrad an.
     - **Informationen:** Zeigt nur Protokolle an, die allgemeine Informationen beschreiben.
     - **Fehler:** Zeigt nur Protokolle an, die schwerwiegende Fehler beschreiben, die aufgetreten sind.
     - **Warnungen:** Zeigt nur Protokolle an, die aufgetretene Warnungen beschreiben.
     - **Fehler und Warnungen:** Zeigt nur schwerwiegende Fehler und Warnungen an, die aufgetreten sind.

- **Module:** Lässt Sie das Modul festlegen, für das Sie Protokolle anzeigen möchten. Sie können folgende Moduloptionen angeben:
  - **Alle:** Zeigt Protokolle zu alle Anwendungskomponenten an.
  - **Allgemein:** Zeigt Protokolle zu allgemeinen Prozessen an.
  - **Knoten aus Discovery importieren**: ermöglicht es Ihnen, Protokolle auf aus Discovery importierten Knoten anzuzeigen.
  - **Knoten aus Hypervisor importieren**: ermöglicht es Ihnen, Protokolle auf aus Hypervisor importierten Knoten anzuzeigen.
  - **Knoten aus Datei importieren:** Zeigt nur Protokolle zum Importvorgang von Knoten in die Anwendung aus einer Datei an.
  - **Richtlinienverwaltung:** Zeigt nur Protokolle zur Verwaltung von Richtlinien an.
  - **CA ARCserve Backup-Synchronisation**: Zeigt nur Protokolle über CA ARCserve Backup-Datensynchronisation an.
  - **CA ARCserve D2D-Synchronisation**: Zeigt nur Protokolle über CA ARCserve D2D-Datensynchronisation an.
  - **Aktualisierungen für CA ARCserve D2D**: Zeigt nur Protokolle über in CA ARCserve D2D gemachte Änderungen an.
  - **Aktualisierungen:** Zeigt nur Protokolle zur Aktualisierung der Anwendung an.
  - **CA ARCserve D2D-Sicherungsjobs übergeben:** Zeigt nur Protokolle an, die CA ARCserve D2D-Sicherungsjobs übergeben haben.
  - **Preflight-Check:** Zeigt nur Protokolle zu Preflight-Check-Vorgängen an.
  - **VM-Sicherungsjobs übergeben:** Zeigt nur Protokolle an, die VM-Sicherungsjobs übergeben haben.
- **Knotenname:** Zeigt nur Protokolle für bestimmte Knoten an.

  Hinweis: Dieses Feld unterstützt den Platzhalter '*' und '?'. Geben Sie zum Beispiel 'lod*' ein, um alle Aktivitätsprotokolle für den Computernamen zurückzugeben, der mit 'lod' anfängt.

Hinweis: Die Optionen "Schweregrad", "Module" und "Knotennamen" können zusammen angewendet werden. Sie können beispielsweise Fehler (Schweregrad) anzeigen, die sich auf Aktualisierungen (Module) für Knoten X (Knotenname) beziehen.

Klicken Sie auf "Aktualisieren".

Die Protokollanzeige basiert auf den festgelegten Anzeigeoptionen.

Hinweis: Die angezeigte Zeit basiert auf der Zeitzone, in der sich Ihr CA ARCserve Central Protection Manager-Server befindet.

Links zur Navigationsleiste hinzufügen

Jedes des CA ARCserve Central Applications verfügt in der Navigationsleiste über den Link "Neue Registerkarte hinzufügen". Verwenden Sie diese Funktion, um in der Navigationsleiste Einträge für zusätzliche webbasierte Anwendungen hinzuzufügen, die Sie verwalten möchten. Für jede installierte Anwendung wird automatisch eine neue Verknüpfung zur Navigationsleiste hinzugefügt. Wenn Sie beispielsweise CA ARCserve Central Reporting und CA ARCserve Central Virtual Standby auf "Computer A" installiert haben und CA ARCserve Central Reporting starten, wird CA ARCserve Central Virtual Standby automatisch zur Navigationsleiste hinzugefügt.

Hinweis: Die neu installierten Anwendungen werden nur entdeckt, wenn sich auf demselben Computer eine andere CA ARCserve Central Applications-Anwendung befindet.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste der Anwendung auf den Link "Neue Registerkarte hinzufügen".
2. Geben Sie den Namen und die URL der Anwendung oder Website an, die Sie hinzufügen wollen. Zum Beispiel, www.google.com.

   Geben Sie optional den Speicherort eines Symbols an.
3. Klicken Sie auf "OK".

   Die neue Registerkarte wird dem unteren Ende der Navigationsleiste hinzugefügt.

Beachten Sie Folgendes:

- Die CA Support-Verknüpfung wird Ihnen standardmäßig zur Verfügung gestellt.

Sie können die neue Registerkarte entfernen, indem Sie sie markieren und auf "Entfernen" klicken.

Best Practices

Berücksichtigen Sie Folgendes als Best Practice für die CA ARCserve Central Protection Manager-Anwendung:

- CA ARCserve Central Applications kann mittels Kommunikationen zwischen dem lokalen CA ARCserve Central Applications-Computer und dem Remote-Computer Daten für einen bestimmten Knoten von einem Remote-Computer abrufen.

  Um sicherzustellen, dass der Remote-Zugriff erfolgreich funktioniert, sind die folgenden Beschränkungen erforderlich:

  - **Netzwerkbeschränkung**: Der als "admin$" bezeichnete Remote-Administrator auf dem Administrator-Computer muss aktiviert werden.
  - **Benutzerkontobeschränkung:** Um sich bei CA ARCserve Central Applications anzumelden, verwenden Sie das Bulletin-Administratorkonto vom lokalen CA ARCserve Central Applications-Computer oder die Administratorrechte zum lokalen CA ARCserve Central Applications-Computer und Remote-Computer hinzufügen.

  Hinweis: Um einen Knoten hinzuzufügen, ist es erforderlich, dass Sie die Administratorrechte für den Remote-Computer haben.

- Um einen Knoten nach Knotennamen oder IP-Adresse zu einem Windows Server 2008 R2-Rechner hinzuzufügen, verwenden Sie das Konto auf der Basis einer der folgenden Voraussetzungen:

  - Wenn Sie das Administratorgruppenkonto vom CA ARCserve Central Applications-Computer und den Remote-Computer verwenden, um sich bei CA ARCserve Central Applications anzumelden, können Sie das gleiche Konto verwenden, um einen Knoten hinzuzufügen.
  - Wenn Sie das Bulletin-Administratorkonto vom CA ARCserve Central Applications-Computer verwenden, um sich bei CA ARCserve Central Applications anzumelden, verwenden Sie das Administratorgruppenkonto vom Remote-Computer, um einen Knoten hinzuzufügen.

- Wählen Sie, um Knoten vom Active Directory zu erkennen, eine der folgenden Optionen:

  - Wenn Sie CA ARCserve Central Applications auf einem Knoten installieren, der mit einer Windows-Domäne verbunden ist, erhält CA ARCserve Central Applications Zugriff auf die Active Directory-Informationen, die sich auf dem Domänen-Controller befinden.
  - Wenn Sie CA ARCserve Central Applications auf einem Knoten installieren, der mit einer Arbeitsgruppe verbunden ist, muss folgende Befehlszeile in einem Befehlsfenster ausgeführt werden, um zu bestätigen, dass CA ARCserve Central Applications Zugriff auf den zugeordneten Domänen-Controller hat:

    ```
    nltest /dsgetdc:%domain_name%
    ```

Hinweis: Wenn diese Option mit dem Status ERROR_NO_SUCH_DOMAIN (1355) fehlschlägt, müssen Sie Ihre Netzwerkeinstellungen anpassen.

Ändern des Server-Kommunikationsprotokolls

CA ARCserve Central Applications verwendet standardmäßig Hypertext Transfer Protocol (HTTP) zur Kommunikation zwischen seinen Komponenten. Wenn Ihnen eine sichere Übertragung von Kennwörtern zwischen den Komponenten wichtig ist, wählen Sie das Protokoll Hypertext Transfer Protocol Secure (HTTPS). Wenn Sie dagegen diese zusätzliche Sicherheitsstufe nicht benötigen, können Sie das Protokoll ganz einfach wieder auf HTTP zurücksetzen.

Gehen Sie wie folgt vor:

1. Melden Sie sich über ein Administratorkonto oder ein Konto mit Administratorrechten bei dem Computer an, auf dem die Anwendung installiert ist.

   Hinweis: Wenn Sie sich nicht über ein Administratorkonto oder ein Konto mit Administratorrechten anmelden, konfigurieren Sie die Befehlszeile so, dass sie mit dem Recht "Als Administrator ausführen" ausgeführt wird.

2. Öffnen Sie die Windows-Befehlszeile.

3. Wählen Sie eine der folgenden Vorgehensweisen:

   - **So ändern Sie das Protokoll von HTTP auf HTTPS:**

     Starten Sie das Hilfsprogramm-Tool "changeToHttps.bat" von folgendem Standardspeicherort (der Speicherort des Ordners 'BIN' kann variieren, je nach dem, wo Sie die Anwendung installiert haben):

     ```
     C:\Programme\CA\ARCserve Central Applications\BIN
     ```

     Wenn das Protokoll erfolgreich geändert wurde, wird die folgende Meldung angezeigt:

     ```
     Das Kommunikationsprotokoll wurde auf HTTPS geändert.
     ```

   - **So ändern Sie das Protokoll von HTTPS auf HTTP:**

     Starten Sie das Hilfsprogramm-Tool "changeToHttp.bat" von folgendem Standardspeicherort (der Speicherort des Ordners 'BIN' kann variieren, je nach dem, wo Sie die Anwendung installiert haben):

```
C:\Programme\CA\ARCserve Central Applications\BIN
```

Wenn das Protokoll erfolgreich geändert wurde, wird die folgende Meldung angezeigt:

```
Das Kommunikationsprotokoll wurde auf HTTP geändert.
```

4. Starten Sie den Browser neu und stellen Sie die Verbindung zu CA ARCserve Central Applications neu her.

   Hinweis: Wenn Sie das Protokoll auf HTTPS ändern, wird im Webbrowser eine Warnung angezeigt. Dieses Verhalten tritt wegen eines selbstsignierten Sicherheitszertifikats auf, das Sie auffordert, die Warnung zu ignorieren und fortzufahren, oder dieses Zertifikat zum Browser hinzuzufügen, um dieser Warnung künftig vorzubeugen.

Kapitel 5:
CA ARCserve Central Protection Manager mit IT-Verwaltungsserver-Tools integrieren

Dieses Kapitel enthält folgende Themen:

Integration von CA ARCserve Central Protection Manager mit Nimsoft und Kaseya (siehe Seite 171)
So integrieren Sie CA ARCserve Central Protection Manager mit Nimsoft (siehe Seite 173)
So integrieren Sie CA ARCserve Central Protection Manager mit Kaseya (siehe Seite 178)

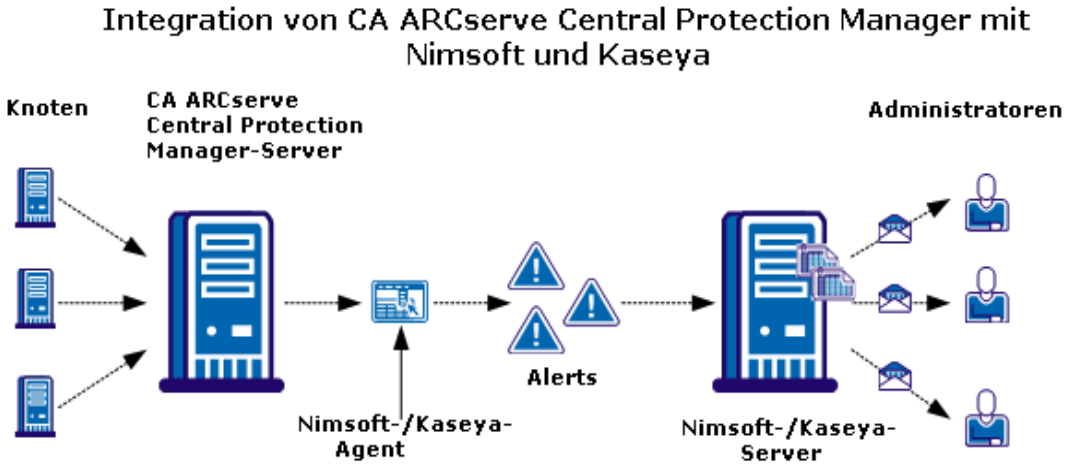
Integration von CA ARCserve Central Protection Manager mit Nimsoft und Kaseya

Sie können so CA ARCserve Central Protection Manager konfigurieren, dass Informationen zu Alert-Meldungen in Echtzeit in den Verwaltungstools für die Infrastruktur von IT-Verwaltungsservern veröffentlicht werden. Durch diese Möglichkeit können die Administratoren der IT-Serververwaltung entsprechend auf CA ARCserve Central Protection Manager-Alerts reagieren.

CA ARCserve Central Protection Manager kann mit folgenden Verwaltungstools für die Infrastruktur von IT-Verwaltungsservern integriert werden:

- Nimsoft
  - Server: 5.11
  - Roboter: 5.32
  - Unified Monitoring Portal: 2.1.2
- Kaseya
  - Server: 6.1.0.0
  - Agent: 6.1.0.6

Das folgende Diagramm veranschaulicht, wie CA ARCserve Central Protection Manager mit Nimsoft und Kaseya integriert werden kann:



Der CA ARCserve Central Protection Manager-Server überwacht Knoten, wo CA ARCserve D2D installiert ist. Wenn der CA ARCserve Central Protection Manager-Server eine Alert-Bedingung entdeckt, sendet er die Alerts an den Nimsoft- oder Kaseya-Agenten, der auf dem CA ARCserve Central Protection Manager-Server installiert ist. Der Agent sendet die Alerts daraufhin unmittelbar zum Nimsoft- oder Kaseya-Server.

CA ARCserve Central Protection Manager überwacht Alerts, die aus den folgenden Anwendungen stammen:

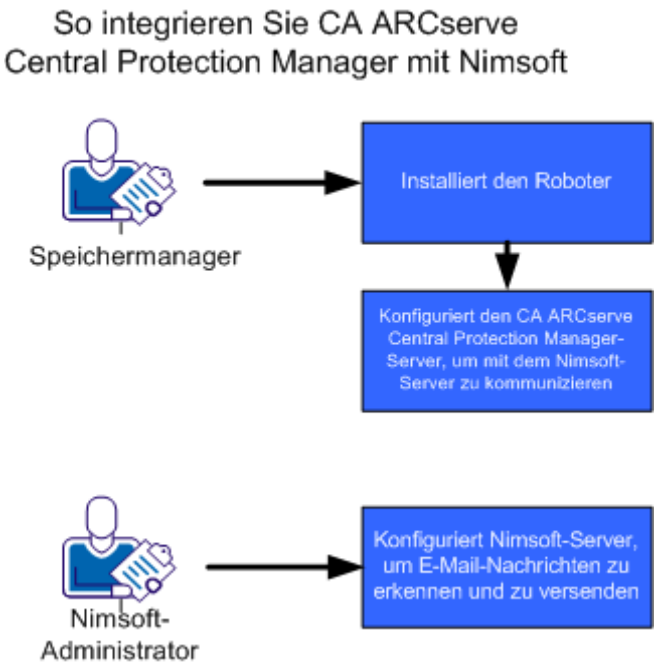
- CA ARCserve D2D
- CA ARCserve Central Virtual Standby
- CA ARCserve Central Host-Based VM Backup
- CA ARCserve Central Protection Manager

Der Nimsoft- oder Kaseya-Server generiert Berichte über Knoten, die diese Anwendungen ausführen. Administratoren können diese Berichte mithilfe der Nimsoft- und Kaseya-Verwaltungstools anzeigen. Nimsoft und Kaseya-Server können so konfiguriert werden, dass die Administratoren auf der Basis vordefinierter Kriterien E-Mail-Nachrichten erhalten.

So integrieren Sie CA ARCserve Central Protection Manager mit Nimsoft

Sicherungs-Manager können CA ARCserve Central Protection Manager so konfigurieren, dass Nimsoft-Server Alert-Meldungen erhalten. Nimsoft-Administratoren können Verwaltungstools der Nimsoft-IT-Infrastruktur so konfigurieren, dass sie CA ARCserve Central Protection Manager-Alerts erkennen, Alert-Berichte generieren und E-Mail-Nachrichten senden. Die Administratoren können die Berichte verwenden, um den Zustand von CA ARCserve D2D-Knoten zu verwalten.

Das folgende Diagramm veranschaulicht, wie Sicherungs-Manager CA ARCserve Central Protection Manager mit Verwaltungstools der Nimsoft-IT-Infrastruktur integrieren:


So integrieren Sie CA ARCserve Central Protection Manager mit Nimsoft
Speichermanager
Installiert den Roboter
Konfiguriert den CA ARCserve Central Protection Manager-Server, um mit dem Nimsoft-Server zu kommunizieren
Nimsoft-Administrator
Konfiguriert Nimsoft-Server, um E-Mail-Nachrichten zu erkennen und zu versenden

Folgen Sie diesen Schritten, um CA ARCserve Central Protection Manager mit Nimsoft zu integrieren:

1. Installieren Sie den Roboter (siehe Seite 174).
2. Konfigurieren Sie den CA ARCserve Central Protection Manager-Server so, dass er mit dem Nimsoft-Server kommuniziert (siehe Seite 175).
3. Konfigurieren Sie Nimsoft-Server so, dass E-Mail-Nachrichten erkannt und gesendet werden. (siehe Seite 176).

Hinweis: Wenn CA ARCserve Central Protection Manager-Server Alert-Meldungen, die lokalisierte Zeichen enthalten, an Nimsoft-Server senden, werden die lokalisierten Zeichen in der Alarmkonsole "Nimsoft Unified Monitoring Portale (UMP)" als unleserlicher Text angezeigt. Konfigurieren Sie, um diesem Verhalten vorzubeugen, den Nimsoft-Server so, dass er UTF-8-Verschlüsselung verwendet. Weitere Informationen finden Sie unter dem Abschnitt "Zeichen aus lokalisierten Servern werden in der Nimsoft UMP-Alarmkonsole als unleserlicher Text angezeigt" im CA ARCserve Central Protection Manager-Benutzerhandbuch.

Installieren des Roboters

Installieren Sie die Option auf dem CA ARCserve Central Protection Manager-Server. Durch den Roboter kann der CA ARCserve Central Protection Manager-Server mit Nimsoft-Servern kommunizieren und ihnen Alert-Meldungen in Echtzeit senden.

Hinweis:]Bevor Sie das Setup-Programm ausführen, sollten Sie überprüfen, ob Sie über eine zulässige Lizenz verfügen.

Gehen Sie wie folgt vor:

1. Laden Sie Setup-Datei des Roboters auf Ihren Computer herunter oder kopieren Sie sie auf Ihren Computer.

   Doppelklicken Sie auf die Datei "*NimBUS Robot.exe*", um die Installation zu starten.

   Das Dialogfeld "Lizenzvereinbarung" wird geöffnet.

2. Klicken Sie auf dem Dialogfeld "Lizenz" auf "Ja", um die Installation zu starten.

   Das Dialogfeld "Zielpfad wählen" wird eingeblendet.

3. Geben Sie den Zielpfad an, unter dem Sie den Roboter installieren wollen, oder klicken Sie auf "Weiter", um das Standardverzeichnis zu akzeptieren.

   Das Dialogfeld "Choose Setup Type" (Setuptyp auswählen) wird geöffnet.

4. Klicken Sie auf "Normale Installation" und danach auf "Weiter".

   Das Dialogfeld "Nimsoft Domain" (Nimsoft-Domäne) öffnet sich und zeigt eine Liste von erkannten Domänen an.

5. Klicken Sie auf das Kontrollkästchen neben der Option "Choose to connect to the network interface through IP address" (Verbindung zur Netzwerkschnittstelle über IP-Adresse auswählen) und klicken Sie auf "Weiter".

   Das Dialogfeld "Specify Nimsoft Hub IP Address" (Nimsoft-Hub-IP-Adresse festlegen) öffnet sich.

6. Geben Sie im Feld für die Hub-IP die IP-Adresse des Nimsoft-Hub an, an den der CA ARCserve Central Protection Manager-Server Alert-Meldungen senden soll.

   Klicken Sie auf "Weiter".

   Das Dialogfeld "Optionen" wird geöffnet.

7. Füllen Sie im Dialogfeld "Optionen" die folgenden Felder aus:

   (Optional) Erster Testport

   Lässt Sie die erste Portnummer festlegen, die verwendet werden soll, wenn Sie Tests starten.

   Hinweis: Legen Sie keinen Port fest, damit das Betriebssystem Zufallsports generiert.

   Passiver Modus

   Geben Sie diesen Modus nur an, wenn der Roboter nicht mit dem Nimsoft-Hub kommunizieren kann. Wenn der Nimsoft-Hub mit dem CA ARCserve Central Protection Manager-Server kommunizieren kann, aktivieren Sie das Kontrollkästchen neben "Passiver Modus".

   Hinweis: Wenn diese Option festgelegt ist, sollten Sie den passiven Roboter der Hub-Konfiguration manuell hinzufügen.

   Klicken Sie auf "Weiter".

   Das Dialogfeld "Start Copying Files" (Kopieren von Dateien starten) wird angezeigt.

8. Klicken Sie auf "Weiter".

   Setup installiert den Roboter.

9. Wenn die Installation abgeschlossen ist, klicken Sie auf "Fertig stellen".

Der Roboter ist installiert.

Konfiguration von CA ARCserve Central Protection Manager-Servern für die Kommunikation mit Nimsoft-Servern

Mit CA ARCserve Central Protection Manager können Sie Alert-Meldungen an Nimsoft-IT-Verwaltungsserver senden. Um die Alert-Informationen zu senden, konfigurieren Sie den CA ARCserve Central Protection Manager-Server für die Kommunikation mit dem Nimsoft-Server.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA ARCserve Central Protection Manager an, und klicken Sie in der Navigationsleiste auf "Konfiguration".

   Die Konfigurationsoptionen werden angezeigt.

2. Klicken Sie in der Konfigurationsliste auf die Option "IT-Management-Server-Konfiguration".

   Die Optionen der "IT-Management-Server-Konfiguration" werden angezeigt.

3. Führen Sie die folgenden Optionen aus:

   a. Klicken Sie auf "Aktivieren".

   b. Klicken Sie auf "Nimsoft".

   c. Geben Sie eine Wiederholungsmethode an. Die Wiederholungsmethode legt die Wochentage fest, an denen Alert-Benachrichtigungen zurück an den Nimsoft-Server gesendet werden sollen, wenn der ursprüngliche Sendeprozess fehlgeschlagen ist. Der Alert-Sendeprozess kann fehlschlagen, wenn der Nimsoft-Server nicht verfügbar oder offline ist.

   d. Geben Sie einen Ablaufplan an. Der Ablaufplan legt die Zeit des Tages fest, an dem die Alert-Benachrichtigungen an den Nimsoft-Server zurück gesendet werden sollen.

   Klicken Sie auf "Speichern".

Der CA ARCserve Central Protection Manager-Server ist so konfiguriert, dass er mit dem Nimsoft-Server kommuniziert.

Konfigurieren des Nimsoft Servers für das Erkennen und Versenden von E-Mail-Nachrichten

Nimsoft-Administratoren können "Alarm SubConsole" so konfigurieren, dass E-Mail-Nachrichten an bestimmte Empfänger gesendet werden, sobald Alert-Meldungen aus CA ARCserve Central Protection Manager-Servern festgestellt werden. Weitere Informationen finden Sie in der Nimsoft-Dokumentation.

Anzeigen von Informationen über Alerts in "Nimsoft Alarm SubConsole"

"Nimsoft Alarm SubConsole" lässt Nimsoft-Administratoren Informationen zu CA ARCserve Central Protection Manager-Alerts anzeigen. "Nimsoft Alarm SubConsole" stellt die folgenden Informationen über CA ARCserve Central Protection Manager-Alerts zur Verfügung:

Hostname

Gibt den Hostnamen des CA ARCserve Central Protection Manager-Servers an, der das Alert an den Nimsoft-Server gesendet hat.

Quelle

Gibt die IP-Adresse des CA ARCserve Central Protection Manager-Servers an, der das Alert an den Nimsoft-Server gesendet hat.

Schweregrad

Gibt den Schweregrad des Alert an, das an den Nimsoft-Server gesendet wurde.

Subsystem

Gibt den Hostnamen des Servers an, der die Alert-Bedingung feststellte.

Beispiel: Die Alert-Bedingung trat auf einem CA ARCserve D2D-Server auf. Das Systemfeld gibt den Hostnamen des CA ARCserve D2D-Servers an.

Subsystem-ID

Gibt die IP-Adresse des Servers an, der die Alert-Bedingung feststellte.

Mit "Alarm SubConsole" können Nimsoft-Administratoren verschiedene Aufgaben ausführen, zum Beispiel Folgende:

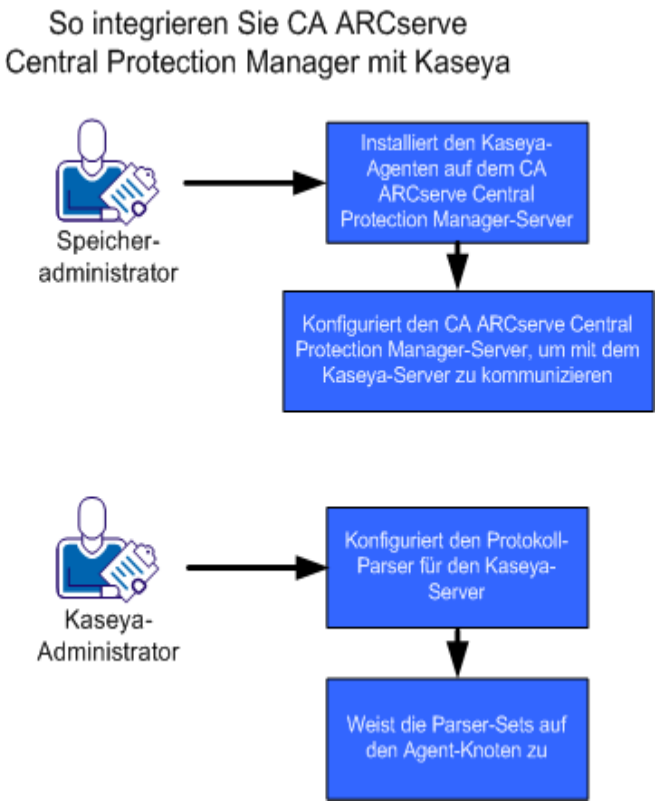
- Konfigurieren Sie "Alarm SubConsole" so, dass E-Mail-Nachrichten an bestimmte Empfänger gesendet werden, sobald Alerts erkannt werden.
- Anzeigen der Alert-Übersicht
- Bestätigen von Alerts
- Alerts Technikern zuweisen

Hinweis: Weitere Informationen über die richtige Verwendung von "Nimsoft Alarm SubConsole" finden Sie in der Nimsoft-Dokumentation.

So integrieren Sie CA ARCserve Central Protection Manager mit Kaseya

Sicherungs-Manager können CA ARCserve Central Protection Manager so konfigurieren, dass Kaseya-Server Alert-Meldungen erhalten. Kaseya-Administratoren können Verwaltungstools der Kaseya-IT-Infrastruktur so konfigurieren, dass sie CA ARCserve Central Protection Manager-Alerts erkennen, Alert-Berichte generieren und E-Mail-Nachrichten senden. Die Administratoren können die Berichte verwenden, um den Zustand von CA ARCserve D2D-Knoten zu verwalten.

Das folgende Diagramm veranschaulicht, wie Sicherungs-Manager CA ARCserve Central Protection Manager mit dem Verwaltungstool der Kaseya-IT-Infrastruktur integrieren:


So integrieren Sie CA ARCserve Central Protection Manager mit Kaseya
Speicher-administrator
Installiert den Kaseya-Agenten auf dem CA ARCserve Central Protection Manager-Server
Konfiguriert den CA ARCserve Central Protection Manager-Server, um mit dem Kaseya-Server zu kommunizieren
Kaseya-Administrator
Konfiguriert den Protokoll-Parser für den Kaseya-Server
Weist die Parser-Sets auf den Agent-Knoten zu

Folgen Sie diesen Schritten, um CA ARCserve Central Protection Manager mit Kaseya zu integrieren:

1. Installieren Sie den Kaseya-Agenten auf dem CA ARCserve Central Protection Manager-Server (siehe Seite 179).
2. Konfigurieren Sie den CA ARCserve Central Protection Manager-Server so, dass er mit dem Kaseya-Server kommuniziert (siehe Seite 180).

3. Konfigurieren Sie den Protokoll-Parser für den Kaseya-Server (siehe Seite 181).
4. Weisen Sie die Parser-Sets auf den Agentenknoten zu (siehe Seite 184).

Installieren des Kaseya-Agenten

Installieren Sie den Kaseya-Agenten auf dem
CA ARCserve Central Protection Manager-Server, damit er mit dem Kaseya-Server kommunizieren kann. Sie installieren den Agenten, indem Sie ihn über die Kaseya-IT-Verwaltungskonsole bereitstellen.

Gehen Sie wie folgt vor:

1. Öffnen Sie ein Browserfenster und melden Sie sich bei der Kaseya-IT-Verwaltungskonsole an.

   Klicken Sie in der Navigationsleiste links im Fenster auf "Agent".

   Die Agentenoptionen werden angezeigt.

2. Erweitern Sie die Option "Install Agents" (Agenten installieren) und auf "Deploy Agents" (Agenten bereitstellen).

   Der Optionen zur Bereitstellung von Agenten werden angezeigt.

3. Aktivieren Sie eine der folgenden Optionen:

   Klicken Sie, um Standardagenten herunterzuladen.

   Damit können Sie die Installationsdatei herunterladen und auf dem Zielcomputer speichern.

   Führen Sie nach dem Herunterladen die Agenteninstallationsdatei direkt auf dem Zielcomputer aus.

   Paket erstellen

   Mit dieser Option können Sie ein Hilfsprogramm für das Installationspaket erstellen, um den Agenten auf einem oder mehreren Computern zu installieren. Folgen Sie den Anweisungen auf dem Bildschirm, um das Installationspaket zu erstellen. Weitere Informationen finden Sie in der Kaseya-Dokumentation.

Der Agent ist installiert.

Konfigurieren Sie den CA ARCserve Central Protection Manager-Server so, dass er mit dem Kaseya-Server kommuniziert.

Mit CA ARCserve Central Protection Manager können Sie Alert-Meldungen an Kaseya-IT-Verwaltungsserver senden. Um die Alert-Informationen zu senden, konfigurieren Sie den CA ARCserve Central Protection Manager-Server für die Kommunikation mit dem Kaseya-Server.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA ARCserve Central Protection Manager an, und klicken Sie in der Navigationsleiste auf "Konfiguration".

   Die Konfigurationsoptionen werden angezeigt.

2. Klicken Sie in der Konfigurationsliste auf die Option "IT-Management-Server-Konfiguration".

   Die Option "IT-Management-Server-Konfiguration" wird angezeigt.

3. Führen Sie die folgenden Optionen aus:

   a. Klicken Sie auf "Aktivieren".

   b. Klicken Sie auf "Kaseya".

   c. Geben Sie eine Wiederholungsmethode an. Die Wiederholungsmethode legt die Wochentage fest, an denen Alert-Benachrichtigungen zurück an den Kaseya-Server gesendet werden sollen, wenn der ursprüngliche Sendeprozess fehlgeschlagen ist. Der Alert-Sendeprozess kann fehlschlagen, wenn der Kaseya-Server nicht verfügbar oder offline ist.

   d. Geben Sie einen Ablaufplan an. Der Ablaufplan legt die Zeit des Tages fest, an dem die Alert-Benachrichtigungen an den Kaseya-Server zurück gesendet werden sollen.

   Klicken Sie auf "Speichern".

Der CA ARCserve Central Protection Manager-Server ist so konfiguriert, dass er mit dem Kaseya-Server kommuniziert.

Konfigurieren Sie den Protokoll-Parser für den Kaseya-Server.

Um Informationen zu CA ARCserve Central Protection Manager-Alerts anzuzeigen, konfigurieren Sie den Kaseya-Server so, dass er Daten in CA ARCserve Central Protection Manager-Alert-Protokolldateien liest.

Gehen Sie wie folgt vor:

1. Öffnen Sie ein Browserfenster und melden Sie sich bei der Kaseya-IT-Verwaltungskonsole an.
2. Klicken Sie in der Navigationsleiste links im Fenster auf "Monitor".

   Die Monitoroptionen werden angezeigt.
3. Erweitern Sie die Option "Log Monitoring" (Protokoll-Monitoring) und klicken Sie auf "Log Parser" (Protokoll-Parser).

   Die Konfigurationsoptionen für Protokoll-Parser werden angezeigt.
4. Klicken Sie in der Liste "Machine.Group ID" auf das Kontrollkästchen neben dem CA ARCserve Central Protection Manager-Server.

   Klicken Sie in der Drop-down-Liste des Felds "Log File Parser" (Protokolldatei-Parser) auf <Select Log Parser> (Protokoll-Parser auswählen).

   Klicken Sie auf "Neu".

   Das Dialogfeld "Log File Parser Definition" (Definition für Protokolldatei-Parser) wird geöffnet.
5. Füllen Sie im Dialogfeld "Log File Parser Definition" die folgenden Felder aus:

   Parser Name

   Definiert den Namen der Datei "Log File Parser".

Log File Path

Definiert den Pfad zur Protokolldatei auf dem CA ARCserve Central Protection Manager-Server. Der Pfad für die Protokolldatei lautet wie folgt:

```
<HOME_CA ARCserve Central Applications>\ITMgmtIntegration\<log_fle_name>
```

CA ARCserve Central Protection Manager generiert Protokolldateien, die Unicode- und Nicht-Unicode-Zeichen unterstützen. Die Protokolldateinamen lauten folgendermaßen:

Nicht-Unicode:

```
CentralAppAlertsForKaseyaANSI.log
```

Unicode:

```
CentralAppAlertsForKaseyaUTF8.log
```

Wichtig! Die Kaseya-IT-Verwaltungskonsole unterstützt Unicode-Zeichen nicht. Verwenden Sie deswegen die Protokolldatei mit Namen "CentralAppAlertsForKaseyaANSI.log".

Log Archive Path

Definiert den Pfad zur archivierten Protokolldatei auf dem CA ARCserve Central Protection Manager-Server. Standardmäßig archiviert Protection Manager die Protokolldatei, wenn ihre Größe 10 MB überschreitet.

Hinweis: Um einen alternativen Wert anzugeben für den Zeitpunkt, zu dem Protection Manager die Protokolldatei archiviert, ändern Sie den Wert für "MaxLogFileSize" (in MB) in folgender Datei:

```
<HOME_CA ARCserve Central Applications>\ITMgmtIntegration\Configuration\Edge-ITMgmtIntegration.INI
```

Beschreibung

Definiert die Beschreibung der Datei "Log File Parser".

Template

Definiert das Format der in der Protokolldatei auf dem CA ARCserve Central Protection Manager-Server enthaltenen Daten. Verwenden Sie die folgende Syntax:

```
$CACentral Protection Manager Machine Name$ [$Alert Generated Product$] $Alert Generated Machine Name$ $Severity$ $Send Time From Origin Product$ $Alert Message$
```

Output Template

Definiert das Format der Ausgabedaten auf dem Kaseya-Server. Verwenden Sie die folgende Syntax:

```
$Protection Manager Server$ $Generated by$ $Host Name$ $Severity$ $Sent$ $Message$
```

Log File Parameters

Erstellen Sie die folgenden Log File Parameters (Protokolldateiparameter):

Hinweis: Klicken Sie auf "Anwenden", nachdem Sie den Typ (von Parameter) angegeben haben, um den Parameter zu speichern.

Computername von CA ARCserve Central Protection Manager

Typ: String

Alert-generiertes Produkt

Typ: String

Alert-generierter Computername

Typ: String

Schweregrad

Typ: String

Sendezeit des ursprünglichen Produkts

Typ: DateTime

Format: YYYY-MM-DD hh:mm:ss

Alert-Meldung

Typ: String

Klicken Sie auf "Speichern".

Die Definition für "Log Parser" (Protokoll-Parser) wurde gespeichert.

6. Klicken Sie auf "Schließen".

Das Dialogfeld "Log Parser Definition" (Definition des Protokoll-Parser) wird geschlossen, und die Datei "Log Parser Definition" wird erstellt und auf den CA ARCserve Central Protection Manager-Server angewendet.

Zuweisen des Parser-Sets auf dem Kaseya-Server

Sie konfigurieren Parser-Sets, um Informationen über CA ARCserve Central Protection Manager-Alerts in der Kaseya-Verwaltungskonsole zu filtern. Die Parser-Sets definieren die Bedingungen, nach denen Sie filtern. Zum Beispiel können Sie die Alerts nach ihrem Schweregrad, nach fehlgeschlagenen Sicherungen und anderem filtern.

Gehen Sie wie folgt vor:

1. Öffnen Sie ein Browserfenster und melden Sie sich bei der Kaseya-IT-Verwaltungskonsole an.
2. Klicken Sie in der Navigationsleiste links im Fenster auf "Monitor".

   Die Monitoroptionen werden angezeigt.
3. Erweitern Sie die Option "Log Monitoring" (Protokoll-Monitoring) und klicken Sie auf "Assign Log Parser" (Protokoll-Parser zuweisen).

   Die Optionen zum Zuweisen von Protokoll-Parser-Sets werden angezeigt.
4. Geben Sie im Abschnitt "Assign log parser sets to selected machines" (Zuweisen des Protokoll-Parser-Sets zu ausgewählten Rechnern), die Alert-Optionen an, die Sie benötigen.
5. Klicken Sie in der Drop-down-Liste "Select log parser" auf den Protokoll-Parser, den Sie den Parser-Sets zuweisen wollen.

   Klicken Sie in der Drop-down-Liste "Define parser sets" (Parser-Sets definieren) auf <New Parser Set>.

   Das Dialogfeld "Edit Parser Set" (Parser-Set bearbeiten) wird geöffnet.
6. Legen Sie im Feld "Parser Set Name" einen Namen für das Parser-Set fest und klicken Sie auf "New" (Neu).

   Die Parsing-Optionen werden angezeigt.

7. Legen Sie die folgenden Werte fest:

   Parser-Spalte

   Definiert den Parameter, nach dem Sie filtern wollen.

   Operator

   Gibt an, wie Sie die im Parameter enthaltenen Daten filtern wollen.

   Parameterdatei

   Gibt den Wert des Parameters an, den Sie filtern wollen.

   Klicken Sie auf "Hinzufügen" und dann auf "Schließen"

   Der Filter wird auf das Parser-Set angewendet und das Dialogfeld "Edit Parser Set" (Parser-Set bearbeiten) wird geschlossen.

   Hinweis: Beispiele zum Festlegen von Parser-Set-Filtern finden Sie unter Beispiele für Parser-Set-Filter.

8. Klicken Sie in der Drop-down-Liste "Select log parser" auf den Protokoll-Parser, den Sie anwenden wollen.

   Klicken Sie in der Drop-down-Liste "Define parser sets" (Parser-Sets definieren) auf das Parser-Set klicken, das Sie erstellt haben.

   Klicken Sie in der Spalte "Machine ID" (Rechner-IDs) auf das Kontrollkästchen neben den Servern, die das Parser-Set übernehmen sollen.

   Klicken Sie auf "Übernehmen".

Der Protokoll-Parser und das Parser-Set wurden zugewiesen.

Beispiele für Parser-Set-Filter

Um Parser-Sets zu erstellen, die nur Alerts filtern, die Fehler enthalten, geben Sie die folgenden Werte an:

Parser-Spalte

Schweregrad

Operator

gleich

Parameterfilter

Fehler

Um Parser-Sets zu erstellen, die alle Alerts ungeachtet des Schweregrads anzeigen, geben Sie folgende Werte an:

Parser-Spalte

Schweregrad

Operator

enthält

Parameterfilter

Fehler, Warnung, Information

Um Parser-Sets zu erstellen, die nur Alerts zu fehlgeschlagenen Sicherungen anzeigen, geben Sie die folgenden Werte an:

Parser-Spalte

Alert-Meldung

Operator

enthält

Parameterfilter

Sicherung, fehlgeschlagen

Konfigurieren Sie Kaseya-Server so, dass E-Mail-Nachrichten erkannt und gesendet werden.

Kaseya-Administratoren können die Verwaltungskonsole so konfigurieren, dass E-Mail-Nachrichten an bestimmte Empfänger gesendet werden, sobald Alert-Meldungen aus CA ARCserve Central Protection Manager-Servern festgestellt werden. Weitere Informationen finden Sie in der Kaseya-Dokumentation.

Informationen zu Alerts im Protokoll-Überwachungsserver des Kaseya-Agenten anzeigen

Der Protokoll-Überwachungsserver des Kaseya-Agenten lässt Sie auf der Basis der Kriterien, die Sie im Protokoll-Parser und im Parser-Set festgelegt haben, Alert-Protokolle anzeigen. Mithilfe der Protokolle können Sie Abhilfemaßnahmen identifizieren und ausführen, um die Alert-Bedingung zu korrigieren.

So zeigen Sie Informationen zu Alerts im Protokoll-Überwachungsserver des Kaseya-Agenten an

1. Öffnen Sie ein Browserfenster und melden Sie sich bei der Kaseya-IT-Verwaltungskonsole an.

   Klicken Sie in der Navigationsleiste links im Fenster auf "Agent".

   Die Agentenoptionen werden angezeigt.

2. Erweitern Sie das Feld "Machine Status" (Rechnerstatus) und klicken Sie auf "Agent Logs" (Agent-Protokolle).

   Die Agent-Protokolle werden rechts im Fenster angezeigt.

3. Klicken Sie in der Liste von Servern auf den Server, für den Sie Informationen anzeigen wollen.

   Klicken Sie auf "Aktualisieren".

Die Informationen zu den Alert-Meldungen werden für den festgelegten Server angezeigt.

Kapitel 6: Fehlerbehebung in CA ARCserve Central Protection Manager

Dieser Abschnitt enthält Informationen zur Fehlerbehebung, mit deren Hilfe Sie Probleme erkennen und lösen können, die bei der Verwendung von CA ARCserve Central Protection Manager möglicherweise auftreten.

Dieses Kapitel enthält folgende Themen:

Beim Hinzufügen von Knoten zeigt eine Fehlermeldung an, dass keine Verbindung zum angegebenen Server möglich ist. (siehe Seite 190)
Leere Webseiten oder JavaScript-Fehler treten auf (siehe Seite 192)
Bei Anmeldung in CA ARCserve D2D-Knoten laden sich Webseiten nicht richtig (siehe Seite 194)
Beim Hinzufügen von Knoten werden ungültige Anmeldeinformationen angezeigt. (siehe Seite 195)
Meldungen zu ungültigen Anmeldeinformationen unter Windows XP (siehe Seite 196)
Fehler wegen verweigerten Zugriffs beim Hinzufügen eines Knotens nach IP/Namen (siehe Seite 197)
Beim Anmeldung in der Anwendung wird ein Zertifikatsfehler angezeigt. (siehe Seite 199)
Fehler beim CA ARCserve Backup-Synchronisationsvorgang (siehe Seite 201)
Fehlschlagen von Vorgängen zur erneuten Bereitstellung von CA ARCserve D2D (siehe Seite 202)
Beheben von Problemen beim Laden von Seiten (siehe Seite 203)
Störzeichen werden in Browser-Fenstern angezeigt, wenn man auf CA ARCserve Central Applications zugreift. (siehe Seite 204)
Knoten werden nach einer Namensänderung nicht mehr im Bildschirm "Knoten" angezeigt (siehe Seite 205)
CA ARCserve Central Protection Manager kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen. (siehe Seite 206)
Nach D2D-Bereitstellung werden Knoten nicht verwaltet (siehe Seite 207)
So legen Sie Ablaufpläne zum Löschen von Knotendaten fest (siehe Seite 207)
CA ARCserve Central Applications-Datenbankdienste starten nicht (siehe Seite 208)

Beim Speichern oder Zuweisen einer Richtlinie auf einen CA ARCserve D2D-Server tritt ein "Multiple Connections"-Fehler auf (siehe Seite 209)
Datensynchronisations- und Richtlinienbereitstellungsvorgänge schlagen fehl (siehe Seite 210)
Fehlernummern der Fehlerbehebung (siehe Seite 211)
Die Verknüpfung zum Hinzufügen neuer Registerkarten wird in Internet Explorer 8 und 9 und in Chrome nicht ordnungsgemäß geöffnet (siehe Seite 212)
Die Verknüpfung zum Hinzufügen neuer Registerkarten, RSS-Feeds und Social Networking-Feedback werden in Internet Explorer 8 und 9 nicht ordnungsgemäß geöffnet (siehe Seite 215)
Zeichen aus lokalisierten Servern werden in der Nimsoft UMP-Alarmkonsole als unleserlicher Text angezeigt (siehe Seite 216)

Beim Hinzufügen von Knoten zeigt eine Fehlermeldung an, dass keine Verbindung zum angegebenen Server möglich ist.

Gültig auf Windows-Plattformen.

Symptom:

Wenn Sie versuchen, Knoten über den Bildschirm "Knoten" hinzuzufügen oder zu verbinden, wird folgende Meldung angezeigt:

```
Es kann keine Verbindung zum festgelegten Server hergestellt werden.
```

Lösung:

Wenn die obige Meldung angezeigt wird, wenn Sie am Bildschirm "Knoten" Knoten hinzufügen möchten, können die folgenden korrigierenden Maßnahmen bei der Problemlösung helfen:

- Stellen Sie sicher, dass der Windows Server-Dienst auf dem CA ARCserve Central Protection Manager-Server und auf dem virtuellen Quellrechner (dem Knoten) ausgeführt wird.
- Stellen Sie sicher, dass auf den Datei- und Druckerfreigabedienst von Windows auf dem CA ARCserve Central Protection Manager-Server und auf dem virtuellen Quellrechner (dem Knoten) eine Windows-Firewallausnahme angewendet ist.
- Stellen Sie sicher, dass auf den Windows-Anmeldedienst nur dann eine Windows-Firewallausnahme angewendet ist, wenn der Knoten kein Mitglied einer Domäne ist. Führen Sie diesen Vorgang sowohl auf dem CA ARCserve Central Protection Manager-Server als auch auf dem virtuellen Quellrechner (dem Knoten) durch.

- Stellen Sie sicher, dass dem Modul "Freigabe und Sicherheit" des lokalen Kontos der Wert "Klassisch" zugeordnet ist. Gehen Sie wie folgt vor, um den Wert "Klassisch" anzuwenden:

  Hinweis: Führen Sie die folgenden Schritte sowohl auf dem CA ARCserve Central Protection Manager-Server als auch auf dem virtuellen Quellrechner (dem Knoten) durch.

  1. Melden Sie sich beim CA ARCserve Central Protection Manager-Server an, und öffnen Sie die Systemsteuerung.
  2. Öffnen Sie in der Systemsteuerung "Verwaltung".
  3. Doppelklicken Sie auf "Lokale Sicherheitsrichtlinie".

     Das Fenster "Lokale Sicherheitsrichtlinie" wird geöffnet.
  4. Erweitern Sie im Fenster "Lokale Sicherheitsrichtlinie" "Sicherheitsoptionen".

     Die Sicherheitsrichtlinien werden angezeigt.
  5. Klicken Sie mit der rechten Maustaste auf "Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten", und klicken Sie im Pop-up-Menü auf "Eigenschaften".

     Das Dialogfeld "Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten" wird geöffnet.
  6. Klicken Sie auf "Lokale Sicherheitseinstellung".

     Wählen Sie aus der Drop-down-Liste "Klassisch - lokale Benutzer authentifizieren sich als sie selbst" aus.

     Klicken Sie auf "OK".

- Stellen Sie sicher, dass der auf die lokalen Richtlinien für die LAN Manager-Authentifizierungsebene angewendete Wert festgelegt wird, um LM & NTLMv2 zu senden. Verwenden von NTLMv2-Sitzungssicherheit, wenn diese verhandelt wurde. Gehen Sie wie folgt vor, um den Wert anzuwenden:

  1. Melden Sie sich beim CA ARCserve Central Protection Manager-Server an, und öffnen Sie die Eingabeaufforderung.

     Führen Sie den folgenden Befehl aus:

     ```
     secpol.msc
     ```

     Das Dialogfeld "Lokale Sicherheitseinstellungen" wird geöffnet.
  2. Wählen Sie lokale Einstellungen aus, und klicken Sie auf die Sicherheitsoptionen.

     Suche nach Netzwerksicherheit: LAN Manager-Authentifizierungsebene.

     Doppelklicken Sie auf die Option.

     Das Dialogfeld "Eigenschaften" wird geöffnet.

3. Wählen Sie die entsprechende Option aus, und klicken Sie auf "OK".

   `Senden Sie LM & NTLMv2 - Verwenden Sie NTLMv2-Sitzungssicherheit, wenn diese verhandelt wurde`

4. Führen Sie in der Eingabeaufforderung folgenden Befehl aus:

   `gpupdate`

Der Wert wird angewendet.

Leere Webseiten oder JavaScript-Fehler treten auf

Gültig für Windows Server 2008- und Windows Server 2003-Betriebssysteme.

Symptom:

Wenn Sie CA ARCserve Central Applications-Websites in Internet Explorer öffnen, werden leere Webseiten angezeigt, oder es treten JavaScript-Fehler auf. Das Problem tritt auf, wenn Internet Explorer unter Windows Server 2008- und Windows Server 2003-Betriebssystemen geöffnet wird.

Dieses Problem tritt unter den folgenden Bedingungen auf:

- Sie verwenden Internet Explorer 8 oder Internet Explorer 9, um Ihre Anwendung anzuzeigen, und der Browser erkennt die URL nicht als vertrauenswürdige Seite an.
- Sie verwenden Internet Explorer 9, um Ihre Anwendung anzuzeigen, und verwenden dabei als Übertragungsprotokoll HTTPS.

Lösung:

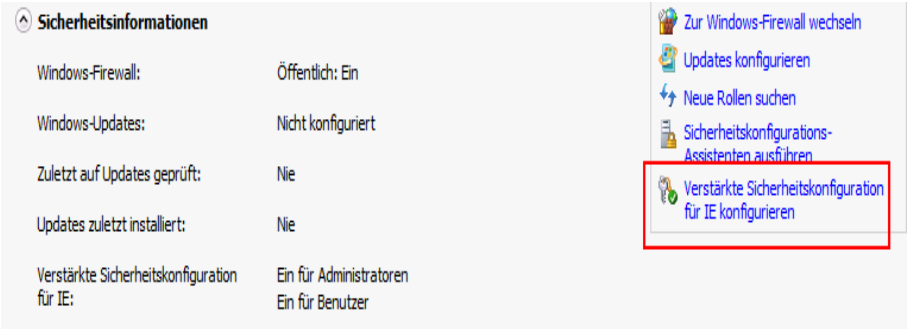
Um dieses Problem zu korrigieren, deaktivieren Sie auf den Computern, die Sie für die Anzeige der Anwendung verwenden möchten, die verstärkte Sicherheitskonfiguration für Internet Explorer.

Um die verstärkte Sicherheitskonfiguration für Internet Explorer unter Windows Server 2008-Systemen zu deaktivieren, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows Server 2008-Computer, den Sie für die Berichtsanzeige verwenden, über das Administratorkonto oder ein Konto mit administrativen Berechtigungen an.
2. Klicken Sie mit der rechten Maustaste auf dem Desktop auf "Computer", und klicken Sie anschließend auf "Verwalten", um das Fenster "Server-Manager " zu öffnen.

3. Klicken Sie im Fenster "Server-Manager " auf "Server-Manager (Servername)".

   Öffnen Sie "Sicherheitsinformationen" im Abschnitt "Serverübersicht", und klicken Sie auf "Verstärkte Sicherheitskonfiguration für IE konfigurieren":



   Das Dialogfeld "Verstärkte Sicherheitskonfiguration für Internet Explorer" wird geöffnet.

4. Gehen Sie im Dialogfeld "Verstärkte Sicherheitskonfiguration für Internet Explorer" folgendermaßen vor:

   - Deaktivieren Sie "Administratoren".
   - Deaktivieren Sie "Benutzer".

   Klicken Sie auf "OK".

Das Dialogfeld "Verstärkte Sicherheitskonfiguration für Internet Explorer" wird geschlossen, und die verstärkte Sicherheit Internet Explorer Sicherheit ist deaktiviert.

Um die verstärkte Sicherheitskonfiguration für Internet Explorer unter Windows Server 2003-Systemen zu deaktivieren, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows Server 2003-Computer, den Sie für die Berichtsanzeige verwenden, über das Administratorkonto oder ein Konto mit administrativen Berechtigungen an.
2. Öffnen Sie die Windows-Systemsteuerung, und öffnen Sie "Software".
3. Klicken Sie im Dialogfeld "Software" auf die Option für Windows-Komponenten "Hinzufügen/Entfernen", um auf den Assistenten für Windows-Komponenten zuzugreifen.

   Entfernen Sie dass das Häkchen neben "Verstärkte Sicherheitskonfiguration für Internet Explorer".

   Klicken Sie auf "Weiter".

   Folgen Sie den Anweisungen auf dem Bildschirm, um die Konfiguration abzuschließen, und klicken Sie auf "Fertig stellen".

Die verstärkte Sicherheit für Internet Explorer wird deaktiviert.

Bei Anmeldung in CA ARCserve D2D-Knoten laden sich Webseiten nicht richtig

Gültig auf Windows-Plattformen.

Symptom:

Webseiten in Browserfenstern laden sich nicht richtig, zeigen Fehlermeldungen an oder beides, wenn man sich vom Bildschirm "Knoten" aus bei CA ARCserve D2D-Knoten anmeldet.

Lösung:

Dieses Verhalten wirkt sich hauptsächlich auf Internet Explorer-Browser aus. Webseiten laden möglicherweise nicht richtig, wenn "Active scripting", ActiveX-Steuerelemente oder Java-Programme auf Ihrem Computer deaktiviert oder auf Ihrem Netzwerk gesperrt sind.

Sie können das Problem durch Aktualisieren Ihres Browserfensters beheben. Wenn das Aktualisieren Ihres Browserfensters das Problem jedoch nicht löst, gehen Sie wie folgt vor:

1. Öffnen Sie den Internet Explorer.

   Klicken Sie im Menü "Extras" auf "Internetoptionen".

   Das Dialogfeld "Internetoptionen" wird geöffnet.

2. Klicken Sie auf die Registerkarte "Sicherheit".

   Die Sicherheitsoptionen werden angezeigt.

3. Klicken Sie auf "Internetzone".

   Die Optionen der Internetzonen werden angezeigt.

4. Klicken Sie auf "Stufe anpassen".

   Das Dialogfeld "Sicherheitseinstellungen - Internetzone" öffnet sich.

5. Blättern Sie bis zur Kategorie "Scripting".

   Suchen Sie "Active Scripting".

   Klicken Sie auf die Option "Aktivieren" oder "Auffordern".

6. Klicken Sie in den Sicherheitseinstellungen auf das Dialogfeld "OK Internetzone".

   Das Dialogfeld "Sicherheitseinstellungen - Internetzone" wird geschlossen.

7. Klicken Sie im Dialogfeld "Internetoptionen" auf "OK".

   Das Dialogfeld "Internetoptionen" wird geschlossen und die Option "Active Scripting" wird angewendet.

Hinweis: Wenn diese Lösung das Problem nicht behebt, setzen Sie sich mit Ihrem Systemadministrator in Verbindung und stellen Sie sicher, dass andere Programme wie Antivirus- oder Firewall-Programme "Active Scripting", ActiveX-Steuerelemente oder Java-Programme nicht blockieren.

Beim Hinzufügen von Knoten werden ungültige Anmeldeinformationen angezeigt.

Gültig auf Windows-Plattformen.

Symptom:

Die folgende Meldung wird angezeigt, wenn Sie versuchen, zum Bildschirm "Knoten" Knoten hinzuzufügen:

```
Ungültige Anmeldeinformationen.
```

Lösung:

Dieses Problem tritt in den folgenden Szenarien auf:

- Die angegebenen Anmeldeinformationen im Dialogfeld "Knoten hinzufügen" sind falsch.
- Die Uhrzeit auf dem Knoten ist nicht die gleiche wie auf dem Anwendungsserver.

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Anwendungsserver und dann bei der Anwendung an.
2. Klicken Sie auf der Startseite in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt:

3. Klicken Sie in der Symbolleiste "Knoten" auf "Hinzufügen", und dann im Pop-up-Menü auf "Knoten nach IP/Namen hinzufügen".

   Das Dialogfeld "Knoten nach IP/Namen hinzufügen" wird geöffnet.

4. Füllen Sie folgende Felder im Dialogfeld "Knoten nach IP/Namen hinzufügen" aus:
   - **IP/Knotenname:** Lässt Sie die IP-Adresse oder den Namen des Knotens festlegen.
   - **Beschreibung:** Lässt Sie eine Beschreibung für den Knoten festlegen.
   - **Benutzername:** Lässt Sie den Windows-Benutzernamen festlegen, der für die Anmeldung beim Knoten erforderlich ist.
   - **Kennwort:** Lässt Sie das Kennwort festlegen, das für die Anmeldung beim Knoten erforderlich ist.

   Klicken Sie auf "Validieren".
5. Wenn die Meldung "Ungültige Anmeldeinformationen" angezeigt wird, gehen Sie wie folgt vor:
   a. Stellen Sie sicher, dass Sie auf dem Dialogfeld "Knoten hinzufügen" die richtigen Anmeldeinformationen angegeben haben und klicken Sie dann auf "Bestätigen".
   b. Wenn die Meldung "Ungültige Anmeldeinformationen" angezeigt wird, stellen Sie sicher, dass die Uhrzeit des Betriebssystems auf dem Anwendungsserver die gleiche ist wie die des Betriebssystems auf dem Knoten.

      Hinweis: Die Uhrzeiten der Betriebssysteme können sich in verschiedenen Zeitzonen befinden. Die Uhrzeiten der Betriebssysteme können nicht unterschiedliche Daten haben. Stellen Sie vor allem sicher, dass das Datum des Betriebssystems auf dem Knoten sich nicht um mehr als einen Kalendertag von dem Datum des Betriebssystems auf dem Anwendungsserver unterscheidet.

Meldungen zu ungültigen Anmeldeinformationen unter Windows XP

Gültig auf Computern mit Windows XP-Betriebssystemen.

Symptom:

Wenn Sie Windows XP-basierte Knoten im Bildschirm "Knoten" hinzufügen, wird die folgende Meldung angezeigt:

```
Ungültige Benutzeranmeldeinformationen.
```

Lösung:

Unter verschiedenen Bedingungen kann CA ARCserve Central Protection Manager keine Windows XP-basierten Knoten hinzufügen, für die "Ordneroptionen" unter "Windows" > "Einfache Dateifreigabe verwenden" aktiviert wurde. Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows XP-Knoten an und öffnen Sie den Windows Explorer.
2. Klicken Sie im Menü "Extras" auf "Ordneroptionen".

   Das Dialogfeld "Ordneroptionen" wird geöffnet.
3. Klicken Sie auf "Anzeigen", und blättern Sie weiter zu "Einfache Dateifreigabe verwenden (empfohlen)".
4. Deaktivieren Sie das Kontrollkästchen neben "Einfache Dateifreigabe verwenden (empfohlen)", und klicken Sie auf "OK".

   Die einfache Dateifreigabe ist nun deaktiviert.
5. Melden Sie sich beim CA ARCserve Central Protection Manager-Server an, und fügen Sie anschließend den Knoten hinzu.

Fehler wegen verweigerten Zugriffs beim Hinzufügen eines Knotens nach IP/Namen

Gültig für alle Windows-Betriebssysteme, die Benutzerkontensteuerung (User Access Control, UAC) unterstützen.

Hinweis: Windows Vista, Windows Server 2008, Windows Server 2008 R2 und Windows 7 unterstützen UAC.

Symptom:

Wenn Sie Knoten über das Dialogfeld "Knoten nach IP/Namen hinzufügen" mithilfe eines neuen Windows-Benutzerkontos hinzufügen, das ein Mitglied der Administratorgruppe ist, wird folgende Meldung angezeigt:

```
Zugriff verweigert. Stellen Sie sicher, dass der Benutzer Administratorrechte hat und der Remote-Registrierungszugriff nicht durch eine lokale Sicherheitsrichtlinie des hinzugefügten Rechners beschränkt ist.
```

Das Ergebnis ist, dass Sie den Knoten nicht hinzufügen können.

Lösung:

Sie können dieses Verhalten erwarten, wenn UAC auf Computern aktiviert ist, auf denen ein Windows-Betriebssystem ausgeführt wird, das UAC unterstützt. UAC ist eine Windows-Funktion, durch die es ausschließlich dem Administratorkonto ermöglicht wird, sich von einem Remote-Standort an dem Computer anzumelden. Die Lösung für dieses Verhalten besteht in den folgenden Schritten:

Gehen Sie wie folgt vor:

1. Melden Sie sich über das Administratorkonto beim Knoten an.
2. Öffnen Sie die Windows-Systemsteuerung.
3. Öffnen Sie die Benutzerkonten.
4. Klicken Sie im Fenster "Änderungen am eigenen Konto durchführen" auf "Einstellungen der Benutzerkontensteuerung ändern", und führen Sie anschließend einen der folgenden Schritte durch:
   - **Windows Vista und Windows Server 2008:** Klicken Sie im Fenster "Änderungen am eigenen Konto durchführen" auf "Benutzerkontensteuerung ein- oder ausschalten" Deaktivieren Sie anschließend im Fenster "Benutzerkontensteuerung einschalten, um den Computer sicherer zu machen" das Kontrollkästchen neben "Benutzerkontensteuerung verwenden, um zum Schutz des Computers beizutragen", und klicken Sie auf "OK".

     Starten Sie Ihren Computer neu, um die Änderungen auf UAC anzuwenden.
   - **Windows Server 2008 r2 und Windows 7:** Schieben Sie im Fenster "Benachrichtigungen über Änderungen an dem Computer auswählen" den Regler von "Immer benachrichtigen" auf "Nie benachrichtigen". Klicken Sie auf OK und schließen Sie die Windows-Systemsteuerung.

     Starten Sie Ihren Computer neu, um die Änderungen auf UAC anzuwenden.

5. Vergewissern Sie sich nach dem Neustart, dass die folgenden Konfigurationen auf den CA ARCserve D2D-Knoten angewandt werden:
   - Der Windows-Server-Dienst wird ausgeführt.
   - Der Datei- und Druckerfreigabedienst darf durch die Windows-Firewall hindurch kommunizieren.
   - Wenn vom Knoten nicht verlangt wird, dass er sich einer Domäne anschließt, darf der Anmeldedienst durch die Windows-Firewall hindurch kommunizieren.
   - Der Wert für "Lokale Sicherheitsrichtlinie", "Lokale Richtlinien", "Sicherheitsoptionen", "Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten" ist "Klassisch".
6. Vergewissern Sie sich, dass die folgende Konfiguration auf den Protection Manager-Server angewandt wird:
   - Der Wert für "Lokale Sicherheitsrichtlinie", "Lokale Richtlinien", "Sicherheitsoptionen", "Netzwerksicherheit: LAN Manager-Authentifizierungsebene" ist "LM- und NTLM-Antworten senden (NTLMv2-Sitzungssicherheit verwenden, wenn ausgehandelt)".

Beim Anmeldung in der Anwendung wird ein Zertifikatsfehler angezeigt.

Gültig auf Windows-Plattformen.

Symptom:

Die folgende Meldung wird in Ihrem Browserfenster angezeigt, wenn Sie sich bei der Anwendung anmelden:

- Internet Explorer:

  ```
  Es gibt ein Problem mit dem Sicherheitszertifikat dieser Website.
  ```

- Firefox:

  ```
  Diese Verbindung ist nicht vertrauenswürdig.
  ```

- Chrome:

  ```
  Dem Sicherheitszertifikat dieser Seite wird nicht vertraut!
  ```

Wenn Sie eine Option angeben, mit der Sie zur Website gelangen, können Sie erfolgreich bei der Anwendung anmelden. Dieses Verhalten tritt jedoch jedes Mal auf, wenn Sie sich bei der Anwendung anmelden.

Lösung:

Dieses Verhalten tritt auf, wenn Sie angeben, dass HTTPS als Kommunikationsprotokoll verwendet werden soll. Um dieses Problem vorübergehend zu korrigieren, klicken Sie in Ihrem Browserfenster auf den Link, mit dem Sie weiter zur Website gelangen. Diese Meldung wird jedoch jedes Mal angezeigt werden, wenn Sie sich bei der Anwendung anmelden.

Das HTTPS-Kommunikationsprotokoll bietet eine höhere Sicherheitsebene als das HTTP-Kommunikationsprotokoll. Wenn Sie weiterhin unter Verwendung eines HTTPS-Kommunikationsprotokolls kommunizieren möchten, können Sie ein Sicherheitszertifikat von VeriSign erwerben und das Zertifikat auf dem Anwendungsserver installieren. Optional können Sie das von der Anwendung verwendete Kommunikationsprotokoll in HTTP ändern. Um das Kommunikationsprotokoll in HTTP zu ändern, gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Server an, auf dem Sie die Anwendung installiert haben.
2. Wechseln Sie zu dem folgenden Verzeichnis:

   ```
   C:\Programme\CA\ARCserve Central Applications\BIN
   ```

3. Führen Sie die folgende Batch-Datei aus:

   ```
   ChangeToHttp.bat
   ```

4. Nachdem die Batch-Datei ausgeführt wurde, öffnen Sie Windows Server Manager.

   Starten Sie den folgenden Dienst neu:

   ```
   CA ARCserve Central Applications Service
   ```

Fehler beim CA ARCserve Backup-Synchronisationsvorgang

Gültig auf Windows-Plattformen.

Symptom:

Der CA ARCserve Backup-Synchronisationsvorgang schlägt fehl und wird im Anzeigeprotokoll angezeigt.

Lösung:

Der CA ARCserve Backup-Synchronisationsvorgang kann fehlschlagen, wenn nicht genügend Festplattenspeicherplatz vorhanden ist, um temporäre Synchronisationsdaten (Speicherauszugsdateien) zu speichern. Standardmäßig speichert die Anwendung die Speicherauszugsdateien im Verzeichnis "ARCserve_Central_Applications_Home\ASBUSync".

Wenn der Speicherplatz auf der Festplatten in C:\Programme begrenzt ist, und die in ASBUSync enthaltenen Dateien mehr Platz in Anspruch nehmen als frei ist, kann die Anwendung die Speicherauszugsdaten der CA ARCserve Backup-Datenbank nicht abrufen, die erforderlich sind, um den Synchronisationsvorgang abzuschließen. Der CA ARCserve Backup-Synchronisationsvorgang schlägt deshalb fehl.

Optional lässt Sie die Anwendung einen alternativen Speicherort angeben, um CA ARCserve Backup-Synchronisationsdaten zu speichern. Um dieses Problem zu beheben oder diesem Problem vorzubeugen, gehen Sie wie folgt vor:

1. Melden Sie sich beim CA ARCserve Central Protection Manager-Server an.
2. Öffnen Sie den Windows-Registrierungs-Editor, und suchen Sie nach Folgendem:

   `HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve Central Application\CM`
3. Klicken Sie mit der rechten Maustaste auf CM, wählen Sie "Neu" aus und klicken Sie im Pop-up-Menü auf "Zeichenfolgewert".

   Benennen Sie den Schlüssel folgendermaßen:

   `ARCserveSyncPath`
4. Klicken Sie mit der rechten Maustaste auf "ARCserveSyncPath", und wählen Sie im Kontextmenü die Option "Ändern" aus.

   Das Dialogfeld "Zeichenfolge bearbeiten" wird geöffnet.
5. Geben Sie im Feld "Wertdaten" den alternativen Speicherort an, an dem Sie die CA ARCserve Backup-Synchronisationsdaten speichern wollen.

   Klicken Sie auf "OK".

Der alternative Speicherort ist festgelegt.

Fehlschlagen von Vorgängen zur erneuten Bereitstellung von CA ARCserve D2D

Gültig auf Windows-Plattformen.

Symptom:

Wenn Sie CA ARCserve D2D erneut auf Knoten bereitstellen, schließt der Bereitstellungsvorgang nicht erfolgreich ab. Dies zeigt sich, wenn eines der folgenden Ereignisse auftritt:

- Eine der folgenden Meldungen wird im "Bereitstellungsstatus" auf dem Dialogfeld "D2D-Bereitstellung" angezeigt:

  `Die Anmeldung des Benutzers war nicht erfolgreich.`

  `Die gleiche Version, eine neuere Version, oder eine Version dieses Produkts, die nicht unterstützt wird, ist auf dem Zielcomputer installiert. Um die aktuelle Version dieses Produkts installieren zu können, müssen Sie die Vorgängerversion auf dem Zielcomputer deinstallieren.`

  `Setup kann Dateien nicht auf den Remote-Rechner kopieren.`

- Der Knoten wird nicht im Fenster "Knoten" angezeigt.
- Der Knoten wird auf der Ansicht "Knoten" mit einem falschen Status angezeigt. Zum Beispiel wird das Symbol auf der Ansicht "Knoten" angezeigt, oder das Symbol wird nicht auf der Ansicht "Knoten" angezeigt.

Lösung:

Diese Ereignisse treten unter den folgenden Bedingungen auf:

- Der CA ARCserve Central Applications-Webservice hält während des Bereitstellungsvorgangs an oder startet neu und der Zielserver wurde nach der Installation von CA ARCserve D2D nicht neu gestartet.
- Der CA ARCserve Central Applications-Server startet während des Bereitstellungsvorgangs neu und der Zielserver wurde nach der Installation von CA ARCserve D2D nicht neu gestartet.

Die Lösung besteht in der Ausführung folgender Aktionen:

1. Melden Sie sich beim D2D-Server an und starten Sie den Server neu.
2. Melden Sie sich bei Central Protection Manager an und vervollständigen Sie eine der folgenden Aufgaben:
   - Wenn der Knoten in der Knotenliste der Ansicht "Knoten" angezeigt wird und der Status nicht korrekt ist, aktualisieren Sie den Knoten.

     Um den Knoten zu aktualisieren, klicken Sie auf den Knoten und danach im Kontextmenü auf "Aktualisieren".
   - Wenn der Knoten nicht in der Knotenliste der Ansicht "Knoten" angezeigt wird, fügen Sie den Knoten manuell hinzu.

     Um den Knoten manuell hinzuzufügen, klicken Sie in der Symbolleiste auf "Hinzufügen" und danach im Kontextmenü auf "Knoten nach IP/Namen hinzufügen".

Beheben von Problemen beim Laden von Seiten

Gültig auf Windows-Plattformen.

Symptom:

Die folgenden Fehlermeldungen werden in Browserfenstern angezeigt, wenn Sie sich bei CA ARCserve Central Applications-, CA ARCserve D2D-Knoten und Überwachungsserver anmelden.

Meldung 1:

```
Fehler auf dieser Webseite können zu Fehlern bei der Ausführung führen.
```

Meldung 2:

```
!
```

Lösung:

Webseiten werden aus verschiedenen Gründen nicht richtig geladen. Die folgende Tabelle beschreibt häufige Gründe und die entsprechenden Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Es gibt Probleme mit dem zugrunde liegenden HTML-Quellcode.	Aktualisieren Sie die Webseite und versuchen Sie es erneut.
Ihr Netzwerk blockiert "Active Scripting", ActiveX oder Java-Programme.	Lassen Sie zu, dass Ihr Browser "Aktive Scripting", ActiveX oder Java-Programme verwendet.

Ursache	Korrekturmaßnahme
Ihre Antivirusanwendung ist so konfiguriert, dass temporäre Internetdateien und heruntergeladene Programme durchsucht werden.	Filtern Sie Ihre Antivirusanwendung so, dass mit CA ARCserve Central Applications-Webseiten in Zusammenhang stehende Dateien aus dem Internet zugelassen werden.
Das auf Ihrem Computer installierte Skriptmodul ist fehlerhaft oder veraltet.	Aktualisieren Sie das Skriptmodul.
Die auf Ihrem Computer installierten Treiber für die Grafikkarte sind fehlerhaft oder veraltet.	Aktualisieren Sie die Treiber für die Grafikkarte.
Die auf Ihrem Computer installierte DirectX-Komponente ist fehlerhaft oder veraltet.	Aktualisieren Sie die DirectX-Komponente.

Störzeichen werden in Browser-Fenstern angezeigt, wenn man auf CA ARCserve Central Applications zugreift.

Gültig auf allen unterstützten Windows-Betriebssystemen. Gilt für alle Browser.

Symptom:

Wenn Sie sich bei CA ARCserve Central Applications anmelden, werden Störzeichen im Inhaltsbereich Ihres Browserfensters angezeigt.

Lösung:

Dieses Problem tritt auf, wenn Sie CA ARCserve Central Applications mithilfe von HTTPS-Kommunikation installieren und dann versuchen, auf CA ARCserve Central Applications mithilfe von HTTP-Kommunikation zuzugreifen. Die zugrunde liegende Webservices-Komponente in CA ARCserve Central Applications unterstützt den Wechsel von HTTP-URLs zu HTTPS-URLs nicht. Dadurch werden Störzeichen in Ihrem Browserfenster angezeigt. Beispiel:

Um dieses Problem zu beheben, greifen Sie mithilfe von HTTPS auf CA ARCserve Central Applications zu, wenn Sie die Anwendungen installieren oder konfigurieren, um mithilfe von HTTPS zu kommunizieren.

Knoten werden nach einer Namensänderung nicht mehr im Bildschirm "Knoten" angezeigt

Gültig auf Windows-Plattformen.

Symptom:

Der Hostname des Knotens wurde geändert, nachdem er zum Fenster "Knoten" hinzugefügt wurde. Der Knoten wird nicht mehr im Fenster "Knoten" angezeigt.

Lösung:

Dieses Verhalten ist normal. CA ARCserve Central Protection Manager behält den Namen des Knotens, der über das Knotenfenster hinzugefügt wurde. Wenn Sie den Knoten umbenennen, kann die Anwendung den Knoten nicht erkennen. Der Knoten wird nicht im Fenster "Knoten" angezeigt.

Um umbenannte Knoten im Fenster "Knoten" anzuzeigen, gehen Sie folgendermaßen vor:

1. Benennen Sie den Knoten um.
2. Öffnen Sie den Bildschirm "Knoten" und löschen Sie den Knoten, (siehe Seite 68) der umbenannt wurde.
3. Knoten hinzufügen (siehe Seite 62) mithilfe seines neuen Namens.

CA ARCserve Central Protection Manager kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen.

Gültig auf Windows-Betriebssystemen.

Symptom:

CA ARCserve Central Protection Manager kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen.

Lösung:

In der folgenden Tabelle wird beschrieben, warum CA ARCserve Central Protection Manager keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen kann, und enthält entsprechende Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Das Netzwerk war bei der Anwendung der Richtlinien nicht verfügbar oder stabil.	Stellen Sie sicher, dass das Netzwerk verfügbar und stabil ist, und versuchen Sie es dann erneut.
Der CA ARCserve D2D-Computer könnte die Arbeitslast nicht verarbeiten, als die Anwendung versuchte, mit dem Knoten zu kommunizieren.	Stellen Sie sicher, dass der CPU auf dem CA ARCserve D2D-Remote-Knoten in einem Normalzustand ist, und versuchen Sie es dann erneut.
Der CA ARCserve D2D-Dienst auf dem Remote-Knoten wurde bei der Anwendung der Richtlinien nicht ausgeführt.	Stellen Sie sicher, dass CA ARCserve D2D auf dem Remote-Knoten ausgeführt wird, und versuchen Sie es dann erneut.
Die Kommunikation des CA ARCserve D2D-Diensts funktionierte nicht richtig.	Starten Sie den CA ARCserve D2D-Dienst auf dem Remote-Knoten neu, und versuchen Sie es dann erneut.

Nach D2D-Bereitstellung werden Knoten nicht verwaltet

Gültig auf Windows-Plattformen.

Symptom:

Wenn ich CA ARCserve D2D auf dem lokalen oder Remote-Server einen Knoten bereitstelle, wird der Knoten der Knotengruppe hinzugefügt aber der Status ist NICHT verwaltet.

Dieses Problem tritt unter folgenden Bedingungen auf:

- CA ARCserve D2D wurde auf einem Remote-Knoten ohne Neustart bereitgestellt.
- CA ARCserve D2D wurde auf einem lokalen CA ARCserve Central Applications-Server ohne Neustart bereitgestellt.

Lösung:

Um dieses Problem zu beheben, starten Sie den CA ARCserve D2D-Server neu und aktualisieren Sie die CA ARCserve D2D-Knoteninformationen in CA ARCserve Central Protection Manager. Der Status wird verwaltet.

So legen Sie Ablaufpläne zum Löschen von Knotendaten fest

Gültig auf Windows-Plattformen.

Symptom:

Standardmäßig wird der Ablaufplan zum Löschen von Knotendaten so festgelegt, dass Daten für gelöschte Knoten jeden Tag um 2:00 gelöscht werden. Ich möchte den Ablaufplan für die Löschung von mehreren Daten anpassen.

Lösung:

Um einen angepassten Ablaufplan für die Löschung von Knotendaten zu erstellen, legen Sie den Wert des Registrierungsschlüssels "CA ARCserve Central Applications\CM\ShowDeleteNodeConfigurationUI" auf 1 fest. Wenn Sie den Registrierungsschlüssel auf 1 setzen, wird im Konfigurationsbereich der CA ARCserve Central Protection Manager-Anwendung die Registerkarte "Konfiguration der Löschung von Knotendaten" hinzugefügt, sodass Sie den Ablaufplan ändern können.

Hinweis: Um auf die Registrierung zuzugreifen, melden Sie sich direkt beim CA ARCserve Central Protection Manager-Server an, und gehen Sie auf Start > Ausführen > Regedit.

CA ARCserve Central Applications-Datenbankdienste starten nicht

Gültig unter Windows-Plattformen, Microsoft SQL Server und Microsoft SQL Server Express Edition-Datenbanken.

Symptom:

Wenn Sie den CA ARCserve Central Protection Manager-Server oder den Server, auf dem die CA ARCserve Central Applications-Datenbank installiert ist, starten oder neu starten, starten die CA ARCserve Central Applications-Datenbankdienste nicht.

Lösung:

Wenn Sie einen Computer starten, berichten Dienste ihren Startstatus dem Betriebssystem. Wenn Dienste ihren Startstatus nicht innerhalb eines vorher festgelegten Zeitraums (oder Zeitlimits) dem Betriebssystem berichten, beendet Windows den Service. Standardmäßig beendet Windows den CA ARCserve Central Applications-Datenbankdienst, wenn die CA ARCserve Central Applications-Dienste nicht innerhalb von 30 Sekunden nach der Startzeit Windows über ihren Status berichten. Es ist wahrscheinlicher, dass Sie auf Probleme dieser Art stoßen, wenn die Datenbank auf einem Server installiert ist, auf dem nicht genügend Ressourcen vorhanden sind. Allerdings können Sie verhindern, dass dieses Problem auftritt, indem Sie das Zeitlimit für die Startdauer erhöhen. Führen Sie folgende Schritte aus, um das Zeitlimit zu erhöhen:

1. Öffnen Sie den Registrierungs-Editor von Windows und suchen Sie nach dem folgenden Schlüssel:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`
2. Klicken Sie mit der rechten Maustaste auf "Steuerelement", zeigen Sie auf "Neu" und klicken Sie im Kontextmenü auf "Schlüssel".

   Ein Schlüssel mit Namen "Neuer Schlüssel #1" wird erstellt.
3. Ersetzen Sie den Eintrag "Neuer Schlüssel #1" durch "ServicesPipeTimeout".
4. Klicken Sie mit der rechten Maustaste auf "ServicesPipeTimeout", und wählen Sie im Kontextmenü die Option "Ändern" aus.

   Das Dialogfeld "DWORD-Wert bearbeiten" wird geöffnet.
5. Geben Sie im Feld "Wertdaten" den Wert an, den Sie für das Zeitlimit festlegen wollen. Drücken Sie den Wert in Millisekunden aus. Um das Zeitlimit zum Beispiel auf 60 Sekunden festzulegen, geben Sie im Feld "Wertdaten" 60000 ein.

   Hinweis: Eine Sekunde entspricht 1000 Millisekunden.

   Klicken Sie auf "OK".

   Die Zeitlimitdauer wird angewendet.
6. Um die Änderungen auf Windows anzuwenden, starten Sie den Computer neu.

Beim Speichern oder Zuweisen einer Richtlinie auf einen CA ARCserve D2D-Server tritt ein "Multiple Connections"-Fehler auf

Gültig für alle Windows-Plattformen.

Symptom:

Wenn Sie versuchen, eine Richtlinie auf einem CA ARCserve D2D-Server zu speichern oder sie ihm zuzuweisen, wird die folgende Fehlermeldung angezeigt:

```
Validieren des Sicherungsziels ist fehlgeschlagen. Mehrere Verbindungen zu einem Server oder eine freigegebene Ressource vom gleichen Benutzer mithilfe mehr als eines Benutzernamens zu verwenden, ist nicht zulässig. Trennen Sie alle vorherigen Verbindungen zum Server oder freigegebene Ressourcen und versuchen Sie es erneut.
```

Lösung:

Falls die vorausgehende Meldung angezeigt wird, wenn Sie versuchen, eine Richtlinie auf einem CA ARCserve D2D-Server zu speichern oder sie ihm zuzuweisen, können Ihnen die folgenden Korrekturmaßnahmen dabei helfen, das Problem zu lösen:

- Geben Sie das Feld "Benutzernamen" mit "Rechnername (oder Domänenname)\Benutzername" an.
- Gehen Sie zum Remote-Server, auf dem der freigegebene Ordner gehostet wird, und löschen Sie alle Sitzungen aus dem CA ARCserve Central Applications-Server oder CA ARCserve D2D-Server. Wählen Sie eine der folgenden Vorgehensweisen, um die Sitzungen zu löschen:
  - Führen Sie folgende Befehlszeile aus:

    ```
    net session \\machinename /delete
    ```

  - Gehen Sie zum folgenden Verzeichnis, um die Sitzung zu unterbrechen:

    ```
    Compmgmt.msc > Systemprogramme > Freigegebene Ordner > Sitzungen > Sitzung trennen
    ```

- Bestätigen Sie, dass Sie den gleichen Benutzernamen verwenden, um auf den freigegebenen Remote-Ordner zuzugreifen.
- Speichern Sie und stellen Sie die Richtlinie erneut bereit.

Datensynchronisations- und Richtlinienbereitstellungsvorgänge schlagen fehl

Gültig auf Windows-Plattformen.

Symptom:

Die folgende Meldung wird im Aktivitätsprotokoll angezeigt, nachdem der CA ARCserve D2D-Datensynchronisationsvorgang gestartet wurde:

```
Die Anwendung kann sich nicht beim CA ARCserve D2D-Dienst anmelden.
```

Das folgende Meldungsfeld wird angezeigt, wenn Sie eine Richtlinie auf dem Knoten bereitstellen:

```
Bereitstellen der Richtlinie fehlgeschlagen (Fehler beim Erstellen einer Verbindung mit dem Knoten).
```

Lösung:

Dieses Verhalten tritt auf, wenn Sie CA ARCserve D2D auf dem Knoten deinstallieren, nachdem er beim CA ARCserve Central Protection Manager-Server registriert wurde, und CA ARCserve D2D danach manuell neu auf dem Knoten installieren. Dieses Verhalten tritt nicht auf, wenn Sie das Hilfsprogramm zur CA ARCserve Central Protection Manager-Bereitstellung verwenden, um CA ARCserve D2D neu auf dem Knoten zu installieren.

Dieses Verhalten wird vermieden, wenn Sie den Knoten über die Ansicht "Knoten" aktualisieren. Um den Knoten zu aktualisieren, klicken Sie auf den Knoten und danach im Kontextmenü auf "Aktualisieren". Vervollständigen Sie danach die erforderlichen Felder auf dem Dialogfeld "Knoten aktualisieren".

Fehlernummern der Fehlerbehebung

Folgende Tabelle bezeichnet Fehlernummern als Pop-Up-Meldungen, wenn Knoten mithilfe von CA ARCserve Central Protection Manager hinzufügt oder aktualisiert werden.

Fehlernummer	Beschreibung	Lösungsvorschlag
12884901933	Es kann keine Verbindung zum CA ARCserve D2D-Dienst auf *** hergestellt werden, und die Fehlernummer ist 12884901933. Stellen Sie sicher, dass alle Eingaben für den Knoten ist richtig sind und der CA ARCserve D2D-Dienst ausgeführt wird.	Überprüfen Sie Folgendes: ■ Der CA ARCserve D2D-Dienst wird auf dem Knoten ausgeführt. ■ Der Hostname, die IP-Adresse und das Übertragungsprotokoll, die für den Knoten angegeben wurden, sind richtig. ■ Der CA ARCserve D2D-Webservice auf dem Knoten wird ausgeführt und ist nicht gesperrt, da DNS die IP-Adresse nicht für den Knoten auflösen kann. ■ Der CA ARCserve D2D-Webservice auf dem Knoten wird ausgeführt und die Windows-Firewall, oder eine andere Firewall, sperrt nicht die Kommunikation. ■ Das Netzwerkkabel, das mit dem Knoten verbunden ist, funktioniert ordnungsgemäß. ■ Der auf dem Knoten angemeldete Benutzer erhält die erforderlichen Berechtigungen, um über ein drahtloses Netzwerk zu kommunizieren.
12884901935	Es kann keine Verbindung zum CA ARCserve Backup-Dienst auf *** hergestellt werden, und die Fehlernummer ist 12884901935. Stellen Sie sicher, dass alle Eingaben für den Knoten richtig sind und der CA ARCserve Backup-Dienst ausgeführt wird.	Stellen Sie sicher, dass der CA ARCserve Communication Foundation-Dienst auf dem Knoten ausgeführt wird.

Fehlernummer	Beschreibung	Lösungsvorschlag
12884901936	Es kann keine Verbindung zum CA ARCserve Backup-Dienst auf *** hergestellt werden, und die Fehlernummer ist 12884901936. Stellen Sie sicher, dass CA ARCserve Central Applications die Version des CA ARCserve Backup-Dienstes unterstützt, die auf dem Knoten installiert ist.	Überprüfen Sie Folgendes: ■ CA ARCserve Central Applications unterstützt die Version des CA ARCserve Backup-Dienstes, die auf dem Knoten installiert ist. ■ Der CA ARCserve Communication-Dienst wird auf dem Knoten ausgeführt.

Die Verknüpfung zum Hinzufügen neuer Registerkarten wird in Internet Explorer 8 und 9 und in Chrome nicht ordnungsgemäß geöffnet

Gültig für Windows

Symptom:

Wenn ich eine neue Registerkartenverknüpfung unter Angabe einer HTTPS-URL hinzufüge, wird folgende Fehlermeldung angezeigt, wenn ich auf die neue Registerkarte klicke:

- Internet Explorer 8 oder 9:

  ```
  Der Inhalt wurde geblockt, da er nicht mit einem gültigen Sicherheitszertifikat signiert wurde.
  ```

- Chrome:

  ```
  The webpage is not available.
  ```

Lösung:

Um dieses Problem für Internet Explorer zu beheben, gehen Sie folgendermaßen vor:

- Internet Explorer 8

  Klicken Sie auf die Statusleiste, und aktivieren Sie "Geblockte Inhalte anzeigen".

- Internet Explorer 9

  Klicken Sie auf der Statusleiste im unteren Bereich der Seite auf die Schaltfläche "Inhalt einblenden". Die Seite wird aktualisiert, und die hinzugefügte Registerkartenverknüpfung funktioniert.

Um dieses Problem für Chrome zu beheben, gehen Sie folgendermaßen vor:

Schritt 1 - Zertifikat exportieren:

1. Öffnen Sie eine neue Registerkarte in Chrome, und geben Sie die HTTPS-URL ein.

   Folgende Warnmeldung wird angezeigt: "Das Sicherheitszertifikat der Website ist nicht vertrauenswürdig!"

2. Klicken Sie im Adressbalken auf das mit einem "X" versehene Schlosssymbol.

   Ein Pop-up-Fenster mit einer Verknüpfung namens "Zertifikatinformationen" wird geöffnet.

3. Klicken Sie auf die Verknüpfung "Zertifikatinformationen".

   Das Dialogfeld "Certificate" wird geöffnet.

4. Klicken Sie auf die Registerkarte "Details"und anschließend auf "Copy to File", um das Zertifikat auf Ihrem lokalen Computer zu speichern.

   Das Dialogfeld "Certificate Export Wizard" wird geöffnet.

5. Klicken Sie auf "Next", um das Format auszuwählen, das Sie verwenden möchten, um die Datei zu exportieren.

   Hinweis: Standardmäßig ist DER encoded binary X.509 (.CER) aktiviert.

6. Klicken Sie auf "Next", um nach einem Speicherort zu suchen, an dem Sie das Zertifikat speichern möchten.

7. Klicken Sie auf "Next", um den Zertifikatsexport-Assistenten abzuschließen, und anschließend auf "Finish".

Das Zertifikat ist nun erfolgreich exportiert.

Schritt 2 - Zertifikat importieren:

1. Öffnen Sie die Tools-Optionen von Chrome.

   Das Dialogfeld "Options" wird geöffnet.

2. Wählen Sie die Option "Details", und klicken Sie neben "HTTPS/SSL" auf Zertifikate verwalten".

   Das Dialogfeld "Certificates" wird geöffnet.

3. Klicken Sie auf "Import".

   Das Dialogfeld "Certificate Import Wizard" wird geöffnet.

4. Klicken Sie auf "Next", um nach dem Zertifikat zu suchen, das Sie auf Ihrem lokalen Computer gespeichert haben.

5. Klicken Sie auf "Next", um den Zertifikatspeicher ("Certificate Store") zu öffnen.

   Das Dialogfeld "Certificate Store" wird geöffnet.

6. Klicken Sie auf "Browse", um das Dialogfeld "Select Certificate Store" zu öffnen.

   Das Dialogfeld "Select Certificate Store" wird angezeigt:

7. Wählen Sie in der Dateiliste "Trusted Root Certification Authorities", und klicken Sie auf "OK".

   Das Dialogfeld "Certificate Store" wird angezeigt:

8. Klicken Sie auf "Next", um den Zertifikatsimport-Assistenten abzuschließen, und anschließend auf "Finish".

   Es wird eine Sicherheitswarnung angezeigt, die Sie informiert, dass Sie gerade ein Zertifikat installieren.

   Klicken Sie auf "Yes", um den Bedingungen zuzustimmen.

Die Zertifikat wurde erfolgreich importiert.

Die Verknüpfung zum Hinzufügen neuer Registerkarten, RSS-Feeds und Social Networking-Feedback werden in Internet Explorer 8 und 9 nicht ordnungsgemäß geöffnet

Gültig für Windows

Symptom:

Für eine HTTPS-URL einer CA ARCserve Central Applications-Anwendung:

Wenn ich eine neue Registerkartenverknüpfung unter Angabe einer HTTPS-URL zur Navigationsleiste hinzufüge, wird folgende Fehlermeldung angezeigt, wenn ich auf die neue Registerkarte und die Verknüpfung "Feedback" klicke:

```
Die Navigation zu der Webseite wurde abgebrochen.
```

Außerdem werden die RSS-Feeds nicht angezeigt.

Hinweis: Die Verknüpfung "Feedback" zeigt die Fehlermeldung auch dann an, wenn Sie die neu hinzugefügte Registerkartenverknüpfung nicht auswählen.

Lösung:

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

- Internet Explorer 8

  Nachdem Sie sich angemeldet haben, klicken Sie in der Pop-up-Sicherheitswarnmeldung "Möchten Sie nur die Webseiteninhalte anzeigen, die über eine sichere Verbindung übermittelt wurden?" auf "Nein". Dadurch erlauben Sie ungesicherte Inhalte für Ihre Website.

- Internet Explorer 9

  Klicken Sie auf der Statusleiste im unteren Bereich der Seite auf die Schaltfläche "Gesamten Inhalt anzeigen". Die Seite wird aktualisiert, und die hinzugefügte Registerkartenverknüpfung funktioniert.

Zeichen aus lokalisierten Servern werden in der Nimsoft UMP-Alarmkonsole als unleserlicher Text angezeigt

Gültig für Windows

Symptom:

In Alert-Meldungen enthaltene Zeichen, die aus lokalisierten Servern kommen, werden in der Alarmkonsole "Nimsoft Unified Monitoring Portal (UMP)" als unleserlicher Text angezeigt.

Lösung:

Dieses Verhalten tritt auf, wenn der Zeichensatz auf dem Server, der die Alert-Meldungen sendet, nicht mit dem Zeichensatz übereinstimmt, der auf dem Nimsoft-Server ausgeführt wird. Die Lösung zu diesem Problem besteht darin, den Nimsoft-Server so zu konfigurieren, dass er UTF-8-Verschlüsselung verwendet. Um den Nimsoft-Server so zu konfigurieren, dass er UTF-8-Verschlüsselung verwendet, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass das Dashboard-Modul so konfiguriert ist, dass es "–Dfile.encoding=utf-8" als Startparameter verwendet.
2. Stellen Sie sicher, dass die Option für die Argumente von Wasp Extra Java VM als –Dfile.encoding=utf-8 festgelegt ist.

Hinweis: Weitere Informationen finden Sie in der Nimsoft-Dokumentation.

Index

8

Die Verknüpfung zum Hinzufügen neuer Registerkarten, RSS-Feeds und Social Networking-Feedback werden in Internet Explorer - 215

A

Aktualisieren von Knoten - 66
Aktualisieren von Knoten und Richtlinien nach einer Änderung des Hostnamens des CA ARCserve Central Applications-Servers - 70
Ändern des Administratorkontos - 42
Ändern des Server-Kommunikationsprotokolls - 168
Ändern von Knotengruppen - 79
Änderungen in der Dokumentation - 4
Anmelden bei CA ARCserve D2D-Knoten - 69
Anwenden von CA ARCserve Backup-Datensynchronisations-Ablaufplänen - 75
Anzeigen von CA ARCserve Central Protection Manager-Protokollen - 164
Anzeigen von Informationen über Alerts in - 176
Anzeigen von Jobstatusinformationen - 143
Aufbau des Fensters - 58
Auswirkungen des Installationsprozesses auf das Betriebssystem - 28

B

Bearbeiten oder Kopieren von Richtlinien - 137
Beheben von Problemen beim Laden von Seiten - 203
Bei Anmeldung in CA ARCserve D2D-Knoten laden sich Webseiten nicht richtig - 194
Beim Anmeldung in der Anwendung wird ein Zertifikatsfehler angezeigt. - 199
Beim Hinzufügen von Knoten werden ungültige Anmeldeinformationen angezeigt. - 195
Beim Hinzufügen von Knoten zeigt eine Fehlermeldung an, dass keine Verbindung zum angegebenen Server möglich ist. - 190
Beim Speichern oder Zuweisen einer Richtlinie auf einen CA ARCserve D2D-Server tritt ein - 209
Beispiele für Parser-Set-Filter - 185
Bereitstellen von CA ARCserve D2D auf Knoten - 84
Bereitstellen von Richtlinien - 139
Best Practices - 167
Binärdateien mit - 31
Binärdateien mit unrichtigen Informationen zur Dateiversion - 30
Binärdateien ohne eingebettetes Manifest - 30

C

CA ARCserve Central Applications-Bookshelf - 13
CA ARCserve Central Applications-Datenbankdienste starten nicht - 208
CA ARCserve Central Protection Manager automatisch deinstallieren - 26
CA ARCserve Central Protection Manager automatisch installieren - 21
CA ARCserve Central Protection Manager kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen. - 206
CA ARCserve Central Protection Manager mit IT-Verwaltungsserver-Tools integrieren - 171
CA ARCserve Central Protection Manager-Datenbank erneut erstellen - 45
CA ARCserve D2D-Bereitstellungsaufgaben - 83
CA Kontaktieren - 3
CA Technologies-Produktreferenzen - 3

D

Datensynchronisations- und Richtlinienbereitstellungsvorgänge schlagen fehl - 210
Deinstallieren von CA ARCserve Central Protection Manager - 25
Dialogfeld - 61
Die Verknüpfung zum Hinzufügen neuer Registerkarten wird in Internet Explorer 8 und 9 und in Chrome nicht ordnungsgemäß geöffnet - 212
Durchführen einer inkrementellen Synchronisation von CA ARCserve Backup-Daten für einen bestimmten Knoten oder eine bestimmte Knotengruppe - 73
Durchführen einer vollständigen Synchronisation von CA ARCserve Backup-Daten für einen bestimmten Knoten oder eine Knotengruppe - 73

Durchführen einer vollständigen Synchronisation von CA ARCserve D2D-Daten für einen bestimmten Knoten oder eine Knotengruppe - 74

E

Einführung - 11
Einführung in CA ARCserve Central Protection Manager - 11
Erforderliche Installationsaufgaben - 15
Erste Schritte mit CA ARCserve Central Protection Manager - 33
Erstellen von Richtlinien - 88
Exportieren von Knoten in eine Datei - 69

F

Fehler beim CA ARCserve Backup-Synchronisationsvorgang - 201
Fehler wegen verweigerten Zugriffs beim Hinzufügen eines Knotens nach IP/Namen - 197
Fehlerbehebung in CA ARCserve Central Protection Manager - 189
Fehlernummern der Fehlerbehebung - 211
Fehlschlagen von Vorgängen zur erneuten Bereitstellung von CA ARCserve D2D - 202
Festlegen der allgemeinen Voreinstellungen - 125
Festlegen der Dateikopieablaufpläne - 119
Festlegen der Dateikopierichtlinien - 107
Festlegen der Dateikopieziele - 113
Festlegen der Einstellungen für das Kopieren von Wiederherstellungspunkten - 121
Festlegen der E-Mail-Einstellungen - 131
Festlegen der E-Mail-Warnmeldungen - 127
Festlegen der erweiterten Sicherungseinstellungen - 102
Festlegen der Quellen der Dateikopie - 106
Festlegen der Schutzeinstellungen - 89
Festlegen der Voreinstellungen für Aktualisierungen - 133
Festlegen von Cloud-Konfigurations-Details für Dateikopie - 116
Festlegen von Einstellungen vor/nach der Sicherung - 105
Festlegen von Sicherungsablaufplänen - 99
Filtern von Knotengruppen - 87
Funktionen für Knoten - 60
Funktionen für Knotengruppen - 77
Funktionsweise der Anwendung - 12

G

Grundlegende Richtlinie erstellen - 51

H

Hinzufügen von Knoten - 51
Hinzufügen von Knoten durch Importieren virtueller Rechner aus ESX/VC - 64
Hinzufügen von Knoten nach IP-Adresse oder Knotennamen - 62
Hinzufügen von Knoten vom Discovery-Ergebnis - 63
Hinzufügen von Knotengruppen - 77

I

Importieren von Knoten aus einer Datei - 65
Informationen zu Alerts im Protokoll-Überwachungsserver des Kaseya-Agenten anzeigen - 187
Installationshinweise - 17
Installieren des Kaseya-Agenten - 179
Installieren des Roboters - 174
Installieren von CA ARCserve Central Protection Manager - 15, 17
Integration von CA ARCserve Central Protection Manager mit Nimsoft und Kaseya - 171

K

Knoten für die Bereitstellung bearbeiten - 86
Knoten mithilfe von Discovery hinzufügen - 60
Knoten von Bereitstellung löschen - 86
Knoten werden nach einer Namensänderung nicht mehr im Bildschirm - 205
Knoten zu Richtlinien zuweisen - 56
Knoten zur Bereitstellung hinzufügen - 85
Knoteneinstellungen - 75
Konfiguration von CA ARCserve Central Protection Manager-Servern für die Kommunikation mit Nimsoft-Servern - 175
Konfigurieren der Datenbank - 44
Konfigurieren der Einstellungen für die Bereitstellung von D2D - 43
Konfigurieren der Einstellungen von IT-Verwaltungsservern - 38
Konfigurieren des Nimsoft Servers für das Erkennen und Versenden von E-Mail-Nachrichten - 176

Konfigurieren Sie den
CA ARCserve Central Protection Manager-Server so, dass er mit dem Kaseya-Server kommuniziert. - 180
Konfigurieren Sie den Protokoll-Parser für den Kaseya-Server. - 181
Konfigurieren Sie Kaseya-Server so, dass E-Mail-Nachrichten erkannt und gesendet werden. - 186
Konfigurieren von Ablaufplänen für Aktualisierungen von CA ARCserve Central Applications - 39
Konfigurieren von CA ARCserve Backup-Datensynchronisations-Ablaufplänen - 34
Konfigurieren von Discovery-Ablaufplänen - 36
Konfigurieren von E-Mail- und Alert-Einstellungen - 36
Konfigurieren von SRM-Ablaufplänen - 35
Konfigurieren von Voreinstellungen für Social Networking - 41

L

Leere Webseiten oder JavaScript-Fehler treten auf - 192
Links zur Navigationsleiste hinzufügen - 166
Löschen von Knoten - 68
Löschen von Knotengruppen - 81
Löschen von Richtlinien - 138

M

Meldungen zu ungültigen Anmeldeinformationen unter Windows XP - 196
Mithilfe von Discovery nach Knoten suchen - 82

N

Nach D2D-Bereitstellung werden Knoten nicht verwaltet - 207

P

Proxy-Einstellungen konfigurieren - 40

R

Richtlinienkontrolle auf die CA ARCserve D2D-Knoten anwenden - 27

S

Sicherstellen, dass der
CA ARCserve Central Protection Manager-Server mit den Knoten kommunizieren kann - 34
Sicherung jetzt ausführen - 141
So deinstallieren Sie
CA ARCserve Central Protection Manager. - 23
So integrieren Sie
CA ARCserve Central Protection Manager mit Kaseya - 178
So integrieren Sie
CA ARCserve Central Protection Manager mit Nimsoft - 173
So legen Sie Ablaufpläne zum Löschen von Knotendaten fest - 207
So verwalten Sie Knoten in
CA ARCserve Central Protection Manager - 57
Störzeichen werden in Browser-Fenstern angezeigt, wenn man auf CA ARCserve Central Applications zugreift. - 204
Synchronisationsdaten und -optionen - 72

V

Verwalten der Einstellungen der Dateikopie - 105
Verwalten von CA ARCserve D2D-Richtlinien - 88
Verwalten von Sicherungseinstellungen - 89
Verwalten von Voreinstellungen - 125
Verwenden von
CA ARCserve Central Protection Manager - 49
Verwenden von
CA ARCserve Central Protection Manager zur Sicherung von CA ARCserve D2D-Knoten - 50

W

Wiederherstellen von Daten aus Dateien und Ordnern - 152
Wiederherstellen von Daten aus Dateikopien - 148
Wiederherstellen von Daten aus Wiederherstellungspunkten - 145
Wiederherstellen von Daten von virtuellen Rechnern - 155
Wiederherstellen von Knoten in
CA ARCserve Central Protection Manager - 144
Wiederherstellen von Microsoft Exchange-E-Mail-Daten - 160
Wiederherstellen von virtuellen Rechnern an alternativen Speicherorten - 158

Wiederherstellen von virtuellen Rechnern an ursprünglichen Speicherorten - 157

Z

Zeichen aus lokalisierten Servern werden in der Nimsoft UMP-Alarmkonsole als unleserlicher Text angezeigt - 216
Zusammenführungsjob auf einem Knoten unterbrechen - 71
Zusammenführungsjob auf einem Knoten wiederaufnehmen - 72
Zusammenführungsjob-Optionen - 70
Zuweisen des Parser-Sets auf dem Kaseya-Server - 184
Zuweisen und Aufheben der Zuweisung von Knoten aus Richtlinien - 140